Public Safety Statement of Requirements

for Communications & Interoperability

Office for Interoperability and Compatibility
Department of Homeland Security

Volume I, Version 1.2

October 2006

Qualitative

This page intentionally left blank.

Homeland Security
Science and Technology

Command, Control and Interoperability: Communication, Interoperability and Compatibility

Defining the Problem

Emergency responders—police officers, fire personnel, emergency medical services-need to share vital voice and data information across disciplines and jurisdictions to successfully respond to day-to-day incidents and large-scale emergencies. Unfortunately, for decades, inadequate and unreliable communications have compromised their ability to perform mission-critical duties. Responders often have difficulty communicating when adjacent agencies are assigned to different radio bands, use incompatible proprietary systems and infrastructure, and lack adequate standard operating procedures and effective multi-jurisdictional, multi-disciplinary governance structures.

OIC Background

The Department of Homeland Security (DHS) established the Office for Interoperability and Compatibility (OIC) in 2004 to strengthen and integrate interoperability and compatibility efforts to improve local, tribal, state, and Federal emergency response and preparedness. Managed by the Science and Technology Directorate, and housed within the Communication, Interoperability and Compatibility thrust area, OIC helps coordinate interoperability efforts across DHS. OIC programs and initiatives address critical interoperability and compatibility issues. Priority areas include communications, equipment, and training.

OIC Programs

OIC programs, which are the majority of Communication, Interoperability and Compatibility programs, address both voice and data interoperability. OIC is creating the capacity for increased levels of interoperability by developing tools, best practices, technologies, and methodologies that emergency response agencies can immediately put into effect. OIC is also improving incident response and recovery by developing tools, technologies, and messaging standards that help emergency responders manage incidents and exchange information in real time.

Practitioner-Driven Approach

OIC is committed to working in partnership with local, tribal, state, and Federal officials to serve critical emergency response needs. OIC's programs are unique in that they advocate a "bottom-up" approach. OIC's practitioner-driven governance structure gains from the valuable input of the emergency response community and from local, tribal, state, and Federal policy makers and leaders.

Long-Term Goals

- Strengthen and integrate homeland security activities related to research and development, testing and evaluation, standards, technical assistance, training, and grant funding.
- Provide a single resource for information about and assistance with voice and data interoperability and compatibility issues.
- Reduce unnecessary duplication in emergency response programs and unneeded spending on interoperability issues.
- Identify and promote interoperability and compatibility best practices in the emergency response arena.

This page intentionally left blank.

Publication Notice

Abstract

This document contains the assembled requirements for a system of interoperable public safety communications across all local, tribal, state, and Federal "first responder" communications systems.

Change Log

Version	Date	Changes
1.0	March 2004	Initial Document
1.1 Draft	October 2005	A new section describing the network has been added. Minor changes throughout the entire document have been effected. The functional requirements have been reformatted to represent 3 three functional requirements sections, and provides an easier to understand layout that removes redundancies.
1.1	January 2006	Review input and copyedit changes have been incorporated.
1.2	October 2006	Updated Section 3.2, "EMS: Routine Patient Services and Car Crash Scenario," Section 5, "System of Systems," and removed redundant scenarios in Appendix C.
1.2	May 2007	Changed branding from SAFECOM to The Office for Interoperability and Compatibility (OIC). Version and date were not revised since no content changes were made.

Acknowledgements

OIC extends its sincere appreciation to the many public safety practitioners, individuals, and government organizations that directly contributed to the creation of the Public Safety Statement of Requirements (PS SoR) for Communications and Interoperability (C&I).

Contact Information

Please send comments or questions to: S&T-C2I@dhs.gov

This page intentionally left blank.

Introduction

> *"In times of emergencies, the public looks to government, particularly their Public Safety officials, to act swiftly and correctly, and do the things which must be done to save lives, help the injured, and restore order. Most disasters occur without warning, but people still expect a rapid and flawless response on the part of government. There is no room for error. Whether involving a vehicle accident, crime, plane crash, special event, or any other Public Safety activity, one of the major components of responding to and mitigating a disaster is wireless communications. These wireless communications systems are critical to Public Safety agencies' ability to protect lives and property, and the welfare of Public Safety officials."*

This statement comes from the highly regarded *Public Safety Wireless Advisory Committee (PSWAC) Final Report*, presented to the Chairman of the Federal Communications Commission (FCC) and the Administrator of the National Telecommunications and Information Administration (NTIA) in September 1996.[1] The PSWAC Final Report defined and documented critical public safety wireless communication needs in 1996, and projected anticipated needs through the year 2010. The report focused on the requirements for communications resources and the radio frequency spectrum to support those requirements. While the report mentioned the crucial need to promote interoperability, its emphasis was clearly on the necessity of taking immediate measures to alleviate spectrum shortfalls. Fortunately, for public safety and for the benefit of all Americans, the report spurred the allocation of precious spectrum for use by public safety practitioners.

Unfortunately, the communication challenges for those working on the front lines in public safety have not been eliminated. In fact, at a time when more attention is being paid to interoperability among different disciplines and jurisdictions within the community, there still exists fundamental communication deficiencies within disciplines and jurisdictions as practitioners strive to perform the most routine and basic elements of their job functions. Agencies must be "operable," meaning they must have sufficient wireless communications to meet their everyday internal requirements before they place value on being "interoperable," meaning being able to work with other agencies.

This document, the *Public Safety Statement of Requirements (PS SoR) for Public Safety Communications and Interoperability*, is the natural follow-on to the PSWAC Final Report, but differs in three ways, as follows:

- First, the PS SoR is not keyed to the issue of spectrum allocation, but focused on public safety requirements from a broader perspective. Operational and functional requirements delineated in the PS SoR are not based on a particular approach or technology.
- Second, the PS SoR was developed eight years after the PSWAC Final Report was published. While the Final Report did not explicitly identify specific technological approaches along with the stated requirements, it is important to realize that advances in technology have helped to fashion the way practitioners think about their jobs over the years. Because practitioners expect more from technology today, their needs and desires have been affected, sometimes subtly, by industry advances and solutions that exist in today's commercial and consumer world. Additionally, current technological advances promote technically advanced thinking about what the practitioner may be

1. In 1994, the FCC and NTIA established PSWAC to evaluate the wireless communications needs of local, tribal, state, and Federal public safety agencies through the year 2010, as well as to identify problems and to recommend possible solutions.

able to expect 15 years from now. For instance, the possibility that technology refresh cycles could be dramatically reduced for public safety based on these advances is extremely attractive. That said, the methodologies used and the general projections made in the PSWAC Final Report remain as valid today as when they were first published. Based on the rapid changes and potential of technology, the PS SoR addresses current requirements and future requirements for the next 5 to 20 years.

- Third, the PS SoR emphasizes the "information" aspects of communications; that is, the need for the wireless exchange of data, video, and other non-voice mediums. The need for voice communications was clearly made in the PSWAC Final Report, as well as the need for additional bandwidth for other data resources. The PS SoR defines the information requirements of public safety practitioners more explicitly to guide how practitioners will use information resources in the field in mission-critical situations.

Scope

The PS SoR is currently a two-volume set. This volume, Volume I, is qualitative in nature: it describes the public safety environment and the kinds of communication applications and services public safety practitioners might expect to use in the future. Volume II, on the other hand, is quantitative in nature: it provides specific performance requirements and metrics to ensure a quality of service level that is satisfactory or higher for the applications and services identified in Volume I. In addition, Volume II provides specific network performance requirements and metrics to support the applications and services identified in Volume I.

Intended Audience

The PS SoR focuses on the functional needs of public safety first responders—Emergency Medical Services (EMS) personnel, firefighters, and law enforcement officers—to communicate and share information as authorized when it is needed, where it is needed, and in a mode or form that allows the practitioners to effectively use it. The communications mode may be voice, data, image, video, or multimedia, the latter including multiple forms of information.

Because functional requirements are the focus of the PS SoR, it does not specify technologies or business models (i.e., whether requirements should be addressed through owned products and systems or via commercial services). Similarly, the PS SoR does not specify infrastructure, except to note that consistent with first responder operations, it is assumed that terminal links to and from practitioners are wireless unless stated otherwise.

The PS SoR addresses a number of complementary objectives. Most importantly, it is rooted in the goal of improving the ability of public safety personnel to communicate among themselves, with the non-public safety agencies and organizations with whom they work, and with the public that they serve. The PS SoR can also assist the telecommunication interoperability and information-sharing efforts by and among local, tribal, state, and Federal government agencies, and regional entities, by delineating the critical operational functions and interfaces within public safety communications that would benefit from research and development investment and standardization.

The PS SoR can assist Federal programs that work with public safety practitioners to assist wireless interoperability at all government levels to develop a comprehensive vision for public safety communications that satisfies the defined needs. This vision can be reinforced by developing Federal grant

programs that promote government research and development, as well as investment in communications equipment and systems, in a manner consistent with the PS SoR.

The PS SoR provides information that can assist the communications industry to prioritize its research and development investment and product and service development strategies so that they are aligned with public safety communications needs.

The PS SoR is intended to be fully consistent with the National Incident Management System (NIMS)[2] as defined by the Federal Emergency Management Agency (FEMA) in the Department of Homeland Security (DHS). Any inconsistency between this document and NIMS is a discrepancy, and will be addressed in later version of the document.

Finally, the PS SoR can be used to clearly identify public safety operational issues so that discussions regarding existing and proposed regulations and laws can be dealt with expeditiously by regulatory and legislative bodies.

Statement of Requirements Organization

Section 1	**Public Safety Requirements and Roles** defines public safety communication needs and public safety roles and functions. (*See Section 1, "Public Safety Requirements and Roles."*)
Section 2	**Communications Services Definitions** defines communications services—interactive and non-interactive voice communications and interactive and non-interactive data communications. (*See Section 2, "Communications Services Definitions."*)
Section 3	**Public Safety Communications Scenarios** outlines several public safety scenarios based on typical operations to provide a view of future public safety communications. (*See Section 3, "Public Safety Communications Scenarios."*)
Section 4	**Operational Requirements of Public Safety Communications and Interoperability (PS C&I)** identifies the communications operational needs of public safety. (*See Section 4, "Operational Requirements of PS C&I."*)
Section 5	**System of Systems** defines the functional aspects of the system of systems architecture, including defining specific network interfaces. (*See Section 5, "System of Systems."*)

2. Developed by the Secretary of Homeland Security at the request of the President, NIMS integrates effective practices in emergency preparedness and response into a comprehensive national framework for incident management. NIMS will enable responders at all levels to work together more effectively and efficiently to manage domestic incidents no matter what the cause, size or complexity, including catastrophic acts of terrorism and major natural disasters.

Section 6	**Application and Services Functional Requirements** defines the requirements for the application and services, and their feature sets. These feature sets include security, operations, and design methodology. (*See Section 6, "Application and Services Functional Requirements."*)
Section 7	**Public Safety Communications Device Functional Requirements** defines the requirements for the devices on the public safety communications network that transmit and/or receive information on that network. (*See Section 7, "Public Safety Communications Device Functional Requirements."*)
Section 8	**Network Functional Requirements** describes the network functional requirements, or those requirements that are specific to each of the four network hierarchies defined: the Personal Area Network (PAN), the Incident Area Network (IAN, the Jurisdiction Area Network (JAN), and the Extended Area Network (EAN). (*See Section 8, "Network Functional Requirements."*)
Appendix A	**Glossary and Acronyms** lists terminology and acronyms used in this report. (*See Section A, "Glossary and Acronyms."*)
Appendix B	**SAFECOM-AGILE-NIST/OLES Summit** lists the capabilities developed at the SAFECOM-AGILE-NIST (National Institute of Standards and Technology) Summit on Interoperable Communications for Public Safety. (*See Appendix B, "SAFECOM-AGILE-NIST/OLES Summit."*)
Appendix C	**Operational Scenarios** contains a number of additional operational scenarios. (*See Appendix C, "Operational Scenarios."*)
Appendix D	**References** identifies print, standards, and online references of this document. (*See Appendix D, "References."*)

Contents

This page intentionally left blank.

Figures

This page intentionally left blank.

Tables

This page intentionally left blank.

Matrixes

This page intentionally left blank.

1 Public Safety Requirements and Roles

Public safety operations require effective command, control, coordination, communication, and sharing of information with numerous criminal justice and public safety agencies, as well as public utilities, transportation companies, and private industry. Thousands of incidents that require mutual aid and coordinated response occur every day. High-profile incidents, such as bombings or plane crashes, test the ability of public safety service organizations to mount well-coordinated responses. In an era in which technology can bring news, current events, and entertainment to the farthest reaches of the world, many law enforcement officers, firefighters, and emergency medical service (EMS) personnel cannot communicate with each other during routine operations, let alone during major emergencies such as the Oklahoma City Bombing.

There are more than 18,000 law enforcement agencies in the United States. Approximately 95 percent of these agencies employ fewer than 100 sworn officers. Additionally, there are more than 32,000 fire and EMS agencies across the Nation. Due to the fragmented nature of this community, most public safety communications systems are stovepiped, i.e., individual systems that do not communicate with one another or aid in interoperability. Just as the public safety community is fragmented, so is radio spectrum. Public safety radio frequencies are distributed across isolated frequency bands from very high frequency (VHF) (25–50 megahertz (MHz)) to 800 MHz (806–869 MHz), and now 4.9 gigahertz (GHz).

Voice communications are critical, but voice communication requirements are not the only issue. Because of advances in technology, public safety operations are increasingly dependent on the sharing of data, such as images and video. New technologies promote the convergence of information and communications systems with the result that mobile units are increasingly being viewed as merely wireless nodes within information networks.

The public safety community requires interoperable communications, which is the ability to communicate and share information as authorized when it is needed, where it is needed, and in a mode or form that allows the practitioners to effectively use it. Broadly defined, the public safety community performs emergency first-response missions to protect and preserve life, property, and natural resources and to serve the public welfare. Public safety support includes those elements of the public safety community whose primary mission might not fall within the classic public safety definition, but whose mission may provide vital support to the general public or public safety officials. Law enforcement, fire, and EMS fit the first category, while transportation or public utility workers fit the second.

Tables 1 through 3 list components of the public safety community and their primary functions. These tables are incomplete and not meant to be exhaustive.

Table 1: First Responder: Roles and Functions

First Responders	
Community Element	Functions
Emergency Medical Services	Public protection, public health, emergency medication/medical services

Table 1: First Responder: Roles and Functions (Continued)

First Responders	
Community Element	Functions
Fire Services (fire marshal, volunteer and professional fire protection districts, etc.)	Public protection, protection of property, identification of hazardous situations
Law Enforcement (identification services, laboratory, operations, juvenile department, etc.)	Public protection, law enforcement, identification, investigation/evidence gathering, arrest, filing of charges

Table 2: Supplemental Responder: Roles and Functions

Supplemental Responders	
Community Element	Functions
Emergency Management	Public protection, central command and control of public safety agencies during emergencies
Environmental Health/Hazardous Materials specialists, including environmental health personnel	
Homeland Security and Defense Units	
Search and Rescue Teams	
Transportation Personnel	

Table 3: Related Agencies: Roles and Functions

Agencies Related to Public Safety	
Community Element	Functions
Corrections (institution, community corrections, jails, juvenile corrections, etc.)	Inmate welfare, rehabilitation, incarceration, timeliness
Courts (court administrations, judges, bailiffs, court recorders, municipal courts, etc.)	Evidence evaluation, fairness, impartiality, timeliness of judicial system
Defense (public defenders, private attorneys, etc.)	Evidence review, response to charges, suspect's rights, bail recommendation, timeliness, trial preparation
Probation and Parole (parole board, probation officers, etc.)	Reintegration, victim notification, oversight, timeliness
Prosecution (district attorneys, etc.)	Evidence review, prosecution decision, suspect's rights, bail recommendations, trial preparation

2 Communications Services Definitions

This section defines the communications services that public safety agencies require. Digital voice communication is a form of data service. But because voice is the most important communication mechanism for mission-critical operations, it is listed as voice service; all other forms of communications are listed as data services.

It is important to note that over time the definition of mission-critical will remain ever-changing. A variety of factors will contribute to the variability of mission-critical spectrum allocations, technology advances, operational strategy changes, etc. This document will aim to remain consistent with the current understanding of mission-critical communications, reflecting the public safety practitioner understanding, while addressing the technical implications of that understanding.

While this section identifies and discusses the communications services required by today's environment, the demands of tomorrow's first responders may change. Thus this PS SoR is a living document that will define those services as they change or as they become new mission requirements for public safety agencies.

Interactive voice communications between public safety practitioners and their supervisors, dispatchers, members of the task force, etc., require immediate and high-quality response, and must meet much higher performance demands than those required by commercial users of wireless communications. Commands, instructions, advice, and information are exchanged that often result in life-and-death situations for public safety practitioners, as well as for the public.

Non-interactive voice communications occur when a dispatcher or supervisor alerts members of a group about emergency situations or acts to share information, without an immediate response being required or designed in the communications. In many cases, the non-interactive voice communications have the same mission-critical needs as the interactive service.

Data communications are becoming increasingly important to public safety practitioners to provide the information needed to carry out their missions. **Interactive data communications** mean that there is query made and a response provided. Such communications can provide practitioners with maps, floor plans, video scenes, etc. A practitioner need not initiate the query and response; it can include automated queries or responses. A common form of interactive data communications is instant messaging.

Commanders, supervisors, medical staff, etc. can make intelligent decisions more efficiently with data from field personnel. Similarly, personnel entering a burning building armed with information about the building, such as contents, locations of stairwells, hallways, etc., can also perform their duties more efficiently.

Finally, **non-interactive data communications** are one-way streams of data, such as the monitoring of firefighter biometrics and location, etc., which greatly increase the safety of the practitioners. This form of communications also makes command and control easier because a commander is aware of the condition and location of the on-scene personnel.

These types of communications are described in greater detail in Section 3, "Public Safety Communications Scenarios," through examples presented by typical public safety scenarios. The scenarios in the appendix (see Appendix C, "Operational Scenarios.") provide more detail about the communications operational needs of public safety in the three areas of interagency interoperability: day-to-day, task force, and mutual aid.

This page intentionally left blank.

3 Public Safety Communications Scenarios

3.1 Introduction

This section includes four scenarios of typical public safety operations that provide a view of future public safety communications. These scenarios describe credible, realistic incidents, activities, and responses that involve public safety agencies and personnel. While these scenarios do not cover all possible activities and situations, they provide a fairly comprehensive vision of the future of public safety communications. Additional scenarios that depict increasingly complex events and their associated communications requirements are included in Appendix C. In Appendix C, two scenarios—a college football game (a pre-planned event) and a terrorist car bomb—reflect the interaction of multiple services in a local area. Two other scenarios in the appendix—a hurricane and an earthquake—represent service in response to large-scale regional events.

These scenarios have many common elements, which are defined in the following list.

a. **Public Safety Communications Device (PSCD)**—Public safety personnel in these scenarios communicate using PSCDs that are portable (handheld or wearable), unless specifically noted for the command vehicle or other in-vehicle use. A PSCD is a multimode device, meaning that it is capable of communicating on the Personal Area Network (PAN), the Incident Area Network (IAN), and the Jurisdiction Area Network (JAN). PSCDs perform the communications functionality defined in the scenario.

   Because the emphasis of these scenarios is on communications capabilities, other important considerations for technology development, such as form (e.g., how text data is input to the device via keyboard, stylus, or spoken language), are not discussed. The scenarios also do not distinguish whether a public safety individual is carrying one or more such devices; however, it is noted that minimizing the number of separate devices required to provide the described functionality is preferred, consistent with other requirements, such as affordability and maintainability.

b. **Public Safety Communications User Group**—The system recognizes the public safety personnel and resources of a communications user group as sharing communications and information. This implies that traffic related to such a user group traverses only the portion of the network necessary to reach all of its members. Each user group can be a permanent unit or a temporary unit that an authorized user creates for a particular task.

c. **System of Systems**—The communications devices are associated with interconnected systems or networks that range in size from small to large. Whatever their size, systems work with each other to seamlessly pass information and communications back-and-forth. In other words, all systems together become a system of systems as described in detail in Section 5.

d. **Personal Area Network (PAN)**—The PAN for a first responder can take many different forms. Primarily, it is intended to represent a set of devices on the person of a first responder that communicates with the first responder's PSCD as necessary. The devices on a PAN will include such items as heart rate monitors and location sensors. This information could, and would in many cases, be transmitted to other areas of the network. These devices are intended to function as "plug-and-play" devices, i.e., transparent automatic configuration is assumed.

e. **Incident Area Network (IAN)**—An IAN is a network created for a specific incident. This network is temporary in nature. It is typically centered on a wireless access point attached to the first

responder's vehicle, or an IAN node. Multiple vehicles dictate multiple wireless access nodes, all of which coordinate their coverage and transmissions seamlessly and automatically.

f. **Jurisdiction Area Network (JAN)**—The JAN is the main communications network for first responders. It handles any IAN traffic that needs access to the general network, and provides the connectivity to the EAN. This network is more permanent in nature, and is typically made up of JAN nodes, or communications towers. Additionally, it is the component of the network that will handle any and all communications from a first responder PSCD, should a connection with the local IAN fail or be otherwise unavailable.

g. **Extended Area Network (EAN)—**The local systems are in turn linked with county, regional, state, and national systems, known as EANs. It is expected that this network could be both wired and wireless, depending on the type of infrastructure deployed in the area, e.g., microwave point-to-point, fiber.

h. **Permanent and Temporary Networks**—JANs and EANs are networks that exist at all times, whereas the IANs are created on a temporary basis to serve a particular purpose, such as an incident, and then are dissolved. The nature of the IAN is such that it may not reach all areas of an incident. In such cases, the user would either connect to the JAN or create a temporary network using portable radio bridges to extend the IAN to the area not covered.

i. **Public Safety Communications User Registration and Authorization**—User registration and authorization occurs every time a public safety individual begins a work shift and turns on his communications device. The individual needs to provide a positive identification, such as through a biometric scan, to his communications device, which then registers the individual on the network. From that moment on, all voice or data communications from that communications device are associated with that individual only. All the pieces of equipment that can monitor the environment, monitor the health of the individual, locate his exact position, etc. register with the individual's identification on the systems. This is so that every time a monitor provides a measurement, the measured value is associated with that public safety individual.

   Each individual also has privileges, permissions, and authorities to communicate with others and to access databases and systems to complete the individual's work assignments. The systems will allow communications and system access based on the user's profile and authorizations.

j. **Temporary Network Creation and Growth**—An emergency event or incident can happen anywhere. To complete their missions, those responding to the incident must have communications on scene as well as away from the scene for command, control, and information. As public safety individuals and resources, such as ambulances, fire engines, or police cars, respond to an incident, the incident communications system or IAN will automatically recognize the new entry, register and authorize the resource, and allow an authorized user to assign the resource to user groups for communications and information exchange. Additionally, in the absence of a network, such as an IAN or JAN, the communications system is designed to allow continued operation by using a mobile ad hoc network.

The scenarios in sections 3.2, 3.3, and 3.4 relate to future communications capabilities for the first responder. The scenario in Section 3.5 describes future command, control, communications, and information sharing for a large incident

3.2 EMS: Routine Patient Services and Car Crash Scenario

3.2.1 Initial Work Shift Tasks

1. At 6:00 a.m., a paramedic and an emergency medical technician (EMT) report for their crew shift. They receive situation updates from the crew going off duty and go to their assigned ambulance, A-1. The partners turn on their PSCDs to begin their system initialization tasks. Their PSCDs are integrated with the ambulance's incident area network (IAN), which allows them to connect to the public safety network when operating outside the ambulance. At power up, all medical devices, including portable and fixed patient-compartment and external video cameras, go through their self tests. The cameras report their status to the vehicle information system and to the medical systems database. The PSCDs complete their network registrations. The ambulance's network links to the medical systems database to register and download updates from the county public health center, DOT traffic control center, hospitals, and elsewhere.
2. The crewmates go through an identity check with their PSCDs. After authenticating their identity, the vehicle information system sets up their profiles on the medical equipment and the PSCDs. PSCD voice-recognition input establishes levels of authorized data access for all crew members across all databases.
3. The crew runs the Required Inventory program to check the quantity of onboard medical supplies. They restock supplies identified by the system as insufficient. When the system comes on-line, it revises inventory levels for each tagged item taken out or brought into the ambulance. The EMT performs a Vehicle Status check through his PSCD. The system checks and reports each vehicle system, fluid level, and tire inflation level.
4. At 6:25 a.m., the A-1 network notifies the dispatcher via the JAN that its crew is active and available for calls. The dispatcher acknowledges that A-1 is active, and that dispatch is properly receiving location data from the unit.

3.2.2 Duty Day Begins with Routine Patient Services

1. At 7:00 a.m., the paramedic arrives at the patient's home, contacts Dr. Smith, and sets up the camera to provide the wound video feed. Dr. Smith, the patient, and the paramedic briefly discuss the wound, the paramedic re-bandages the wound per Dr. Smith's direction and draws blood samples.
2. At 8:30, the medical systems database that links all public safety, hospital, transportation, and other agencies with access to it, shows the paramedic's status as returning in the I-2 vehicle to the ambulance base for fuel and then to the health clinic. It shows his partner as going to the health clinic to assist the physician's assistant with patients.

3.2.3 EMS Response to Car Crash

1. At 8:40 a.m., a call center for in-vehicle safety systems notifies County dispatch of an accident 12 miles southwest of Bayport. The call center is unable to contact the occupants. The data indicates two occupants involved in a 50 mile-per-hour (MPH) head-on collision and roll-over. The belted driver remains in the front seat. A thrown passenger is in the back seat. The center reports an "urgency" alert derived from the onboard sensors for one severely injured occupant, while the

other occupant is likely less injured. Based on this information, EMS is dispatched immediately. Police and a wrecker are also dispatched.

2. The EMS partners, in A-1 and I-2, access their computers to request the best route to the crash scene, given their current positions and traffic conditions. County dispatch sends a second ambulance, A-3, as well as fire department extrication equipment and personnel All responders dispatched are added to the IAN and Public Safety Communications User Group (PSCUG) for this incident, and their information is updated to reflect who is responding. A-1 adds the Fisherville Emergency Room (ER) to the IAN and PSCUG. (Closest to the crash site, it is Bayport's local medical direction facility.) The EMT also verifies that the Fisherville ER, the Med Flight-1 helicopter, and the Central City Hospital Trauma Center have received the crash notification information because of the urgency of the alert. His PSCD shows the EMS partners in A-1 and I-2 are actively monitoring the network regarding this incident.

3. At 8:42 a.m., the paramedic responding in I-2 checks his PSCD, which verifies the crash site on the map display and identifies the best route. As responding units approach traffic lights, onboard signaling systems change the lights to the responder's favor. Another system sends an "emergency vehicle approaching" signal to vehicles ahead. The paramedic uses his PSCD to locate a helicopter landing site a mile from the crash scene, which is now displayed on the PSCD for the helicopter and other responding crew members. The medical systems database shows the status of the backup ambulance, which has an EMT-level crew onboard. The paramedic also sees that a volunteer EMT-Intermediate residing near the crash scene has been added to the IAN and PSCUG, and is responding to the incident.

4. Simultaneously, at the Trauma Center, the Med Flight-1 crew and lead trauma nurse check their PSCDs, which are beeping an alert tone from the crash notification. The "urgency" alert meets the threshold for "auto-launch" of Med Flight-1, and the crew leaves to start and launch the helicopter. The alert also triggers notification of the trauma team. The trauma team's PSCDs are alerted and added to the IAN and PSCUG, and team members head to the operating room or helipad. This information is entered into the medical systems database.

5. At the same time, the triage nurse at the Fisherville Hospital checks her PSCD, which is sounding a crash alarm. She notes that two ambulances are responding, 10 and 15 minutes from the scene, respectively. She sees that the Trauma Center has been put on alert for this crash and that Med Flight-1 is auto-launching to the scene. Her PSCD shows that the Fisherville ER physician is in the sleep room. She adds the ER physician's PSCD into the IAN and PSCUG, alerting him to the incident. He registers for the incident, which updates the medical systems database, and responds to the ER.

6. At 8:52 a.m., A-1 and I-2 arrive at the scene simultaneously. The paramedic examines the two patients—the male driver and the female passenger, both approximately 50-years-old—and verifies a single vehicle crash into a tree, with roll-over. The male patient is semi-coherently responding to voice, has no visible injuries, and is complaining of chest and shoulder pain. The paramedic places wireless vital-sign and EKG devices that he monitors via his PSCD, which sends the data across the IAN into a "patient 1"profile in the medical systems database. The paramedic finds no tangible tenderness in the chest area and suspects the patient has cardiac pain. He states this into his PSCD, which translates the findings into text that also becomes available in the "patient 1" profile.

   The female patient is trapped in the back seat with doors pinned by a collapsed roof. She is unresponsive but breathing, with an open head injury and possible skull fracture. Again, the paramedic places monitoring devices, which send their data into the "patient 2" profile. The paramedic designates that this patient will go to the Trauma Center via the helicopter. The "patient

2" profile is updated to reflect this change and the information is promulgated to all PSCDs on the IAN. The helicopter continues and the Trauma Team sets up the OR for neurosurgery.

7. At 8:57 a.m., a separate PSCUG is established to assess the male patient. The PSCUG links the EMT, the paramedic, a Trauma Center surgeon, a Faith Hospital cardiologist, and the Fisherville Emergency Department (ED) physician. All have seen the results of patient monitoring, the paramedic's assessment, and the treatment. In addition, "patient 1" has provided a personal medical data medallion, and its information has been added to the "patient 1" profile through the paramedic's PSCD. The medallion includes allergy and medication information, and a baseline EKG.

   All devices and the paramedic's assessment clearly indicate that the patient has suffered a heart attack. The Faith Hospital cardiologist issues an immediate alert to the cardiac catheterization team and adds them to the PSCUG. To confirm the absence of any severe injuries, the Trauma Center surgeon orders the paramedic to perform a portable ultrasound body scan, which is sent to the Trauma Center and verifies the absence of major traumatic injury. Based on consultation among the paramedic, the Fisherville Hospital ED physician, the Faith Hospital cardiologist, and the Trauma Center surgeon, the decision is made not to administer a "clot buster" medication in the ambulance, to bypass the Fisherville Hospital, and transport the patient by ground to the Faith Hospital for cardiac catheterization. This information is entered into the medical systems database. The PSCUG is discontinued.

8. At 9:02 a.m., A-3, the volunteer EMT via a private vehicle, and a fire department heavy rescue vehicle arrive. The medical systems database indicates that the helicopter is on the ground at the landing site. The car's roof is cut and removed

9. At 9:12 a.m., A-1 heads to Faith Hospital, 40 miles away. The paramedic and Faith Hospital cardiologist are joined in a new PSCUG. The paramedic performs repeat (12-lead EKGs) to monitor heart attack progression and treatment results. Medications administered en route seem to improve the patient's condition. The "patient 1" profile is updated continuously, but only Faith Hospital staff and the A-1 crew have authority now to access the "patient 1" information.

10. The female patient is collared, boarded, and removed from the car to A-3. This status is entered in the medical systems database, which alerts the Med Flight-1 crew of the impending arrival of the patient at the landing site. The volunteer EMT accompanies the patient and EMT crew to the landing site. The patient receives two IVs and a breathing tube en route to the landing site, while the helicopter medical crew monitors the "patient 2"profile and real-time video of the treatment on their PSCDs.

11. The volunteer EMT is added to a new PSCUG with the helicopter crew, the Fisherville Hospital ED physician, and the Trauma Center trauma surgeon. This is to provide a verbal patient update and to take orders for additional treatments en route to the landing site. A body scan is ordered on the way to the helicopter and transmitted to the Trauma Center and the helicopter crew. Based on consultation among the helicopter crew, the decision is confirmed to continue transport to the Trauma Center.

3.2.4 EMS Communications Summary

Throughout the scenario, the network tracks the ambulances, the paramedic teams, and the patients, and provides geolocation data in real time. All patient information and vitals are recorded through wireless monitors and voice recognition systems, with no reliance on paper reports and notes. All EMS hospital staff orders, as well as treatments by paramedics, are recorded by the hospital and ambulance databases.

All monitors and devices used with the patient are wireless to allow easy patient transport and mobility. All conversations between dispatcher and paramedics and between paramedics and hospital staff are simultaneous discussions via conference call. All patient data is secure to the maximum extent possible, in complete compliance with the Health Insurance Portability and Accountability Act (HIPAA), or its current, equivalent medical privacy policy.

3.3 Fire-Residential Fire Scenario

3.3.1 Initial Work Shift Tasks

1. Three firefighters begin their shift at the Brookside Fire District Station BFD-7. After completing their administrative check-in, they complete their biometric identity check with their PSCDs. After authenticating each firefighter, the system sets up their profiles on their PSCDs and the network, establishes the level of data access that each is authorized to have across available databases. It also initiates personal tracking of each firefighter so that a record can be made of all instructions given to each, and the actions and responses of each firefighter.

   The firefighters initiate the equipment self tests of the vests they will wear during a fire situation. The vests measure each firefighter's pulse rate, breathing rate, body temperature, outside temperature, and [three-axis gyro] and accelerometer data. Each vest also provides geolocation information for the wearer, and measures the available air supply in the firefighter's air tank. The vests have a self-contained PAN that interrogates each of the sensors and monitors. The vest codes the firefighter’s information with the firefighter's ID, and then transmits the data to the firefighter’s PSCD.

2. The firefighters begin their initialization tasks of the fire equipment, the fire engine, E7, and fire ladder, L7, at the station. Each apparatus has sensors to measure water pressure, water flow, water supply, fuel supply, and geolocation. Each apparatus also has its own PAN for interrogating all apparatus monitors. The apparatus codes the apparatus ID with the measured values and geolocation information for routing to the network. After successfully completing all the self tests, the firefighters provide a digital status to the network informing it that they have completed all initial setups and are ready. The fire station network reports to the dispatcher, via the station data systems and onboard data systems, identifying which personnel and equipment are active and available for calls. The station battalion chief follows up with a PSCD voice call with the same message. The dispatcher acknowledges that the BFD-7 station is active, and that dispatch's Geographical Information System (GIS) and CAD system are properly receiving location and status data from the units.

3.3.2 Fire Response to a Residential Fire Call

1. At 3:17 a.m., the Brookside PSAP receives a 911 call from a cab driver that the apartment building at 725 Pine is smoking and appears to be on fire. From the CAD display, the dispatcher finds that the BFD-7 station is available and close to the address. The dispatcher notifies BFD-7 to send E7 and L7, and to send the BFD-7 battalion chief as the fire's incident commander (IC). As E7 is leaving the fire station, firefighter F788 jumps into the vehicle. The vehicle registers for accountability and tracking that F788 has become part of the E7 crew. The dispatcher simultaneously sends a digital message providing the apartment building's address. The dispatcher notifies another Brookside Fire Department, BFD-12, to also send an engine to the fire. By 3:19 a.m., E7, L7, and the IC leave BFD-7 and report their status to the dispatcher. As the IC's command vehicle leaves the station, a nearby PSCD sends the apartment's building plans and the

locations of nearby fire hydrants, the building's water connections, the elevators, and stairwells to all fire vehicles en route, including the command vehicle. The dispatcher sends a reverse 911 call message to all residents of the building, which has eight apartments on each of three floors. The dispatcher alerts the nearest ambulance to proceed to the scene. The local utility is alerted to stand by for communications with the IC at 725 Pine.

2. The E7, L7, and IC drivers view the apartment's address on the cab monitor displays, which also maps the route for the drivers; a computer-activated voice directs the drivers to the appropriate lanes and where to turn. As the fire vehicles approach traffic lights along the route, the onboard signaling system changes the lights in the emergency vehicles' favor and the geolocation system provides the vehicles' location and progress on the dispatcher's CAD display. The onboard system also interrogates the county's transportation system for road closures, blockages, train conflicts, or slow traffic conditions to route the vehicles around impediments and provide the fastest route to the fire.

3. The IC arrives on scene at 3:22 a.m., assesses the situation, noting that smoke and fire are visible, and alerts dispatch that 725 Pine is a working fire. The IC directs the local utility to shut off the gas to 725 Pine. As L7 and E7 arrive and move into position, all fire personnel and equipment are shown on the IC's display. The system automatically sets up the PSCUG for the IC and the fire crews. The fire crews are able to talk continuously with each other, reporting conditions and warning of hazards. Because the apartment building is not large enough to require a built-in wireless IAN for emergency services, the first fire crew into the apartment drops self-organizing wireless IAN radio bridges on each of the floors as it progresses through the building. Soon E12 and the assigned EMS unit arrive on site. The new personnel and equipment are automatically registered with the IAN, and their PSCDs are automatically reprogrammed to operate on the incident's PSCD radio channels and protocols.

4. Several families have already evacuated the building. As firefighters ask for their names and apartment numbers, they use the voice recognition capabilities of their PSCDs to capture the information, and apply an RFID wrist strap to each resident to track their status and location. Other firefighters enter the building to guide survivors out and to rescue those who are trapped. The infrared (IR) cameras on the firefighter's helmets provide the IC a real-time, on-demand view of fire conditions within the building and the location of the hot spots. Additionally, the firefighters monitor the temperature of the surrounding air in their location; this information is directly available to the firefighter, as well as the IC and EMS unit on scene. Other passive sensors, such as hazardous gas detectors, are also operating in the firefighter's PAN. With the IC's guidance, the firefighters search each apartment for survivors and the source of the fire. The IC is able to monitor the location of each firefighter and is aware of which apartments have been searched through the information provided on the displays.

5. The EMS unit outside the apartment monitors the vital signs of all the firefighters in and around the fire scene. The unit alerts the IC that firefighter F725 is showing signs of distress, and the IC orders F725 and his partner F734 out of the building for a check-up with the EMS team.

6. Firefighter F765 pushes his emergency button when he becomes disoriented in the smoke. The IC immediately directs firefighter F788 to his aid by providing F765's location relative to F788 via three-dimensional geolocation information and the floor plan.

7. While the firefighters check every apartment for victims, the main fire is discovered in a second floor apartment kitchen where an electric range is burning. Two adults and two children are discovered in the apartment suffering from smoke inhalation. They are carried outside the building where the EMS unit is ready to take over medical aid. RFIDs are attached to the arms of the victims, and each is given an oxygen tank and mask to help their breathing.

8. While the firefighters put out the fire in apartment 202, the IC checks the display, which shows where the fire personnel are and where all the survivors and rescued individuals live in the apartment building. Two top-floor apartments have not been searched, and the IC moves fire personnel to those apartments. The apartment database indicates an invalid may be living in apartment 321. The firefighters break down the doors of both apartments and in 321 find a bedridden individual, who is in good condition, and a pet dog in the other apartment. Both are taken from the building and outfitted with RFID devices.

9. The fire is brought under control. The IC releases E12, and the IC reconfigures E12's PSCDs for return to the fire station. E7 and L7 wrap up their fire operations, and A34 has to transport one fire victim to the hospital. The IC releases all remaining equipment and gives control to dispatch.

3.3.3 Fire Communications Summary

Throughout the scenario, the fire personnel and equipment, EMS support personnel, and the fire victims are tracked by the network, which provides geolocation information in real time, giving the IC and any other authorized personnel with current accountability of public safety personnel and of the fire's victims. All victim information and vitals are recorded through wireless monitors and voice recognition systems with no reliance on paper reports and notes. All fire personnel and equipment have monitors to measure vital conditions and status, which are reported by the PSCD and IAN to the IC's management system. The management system also has access to city building department databases, which are searched and queried for building information and plans, fire hydrant locations, etc.

3.4 Law Enforcement: Traffic Stop Scenario

3.4.1 Initial Work Shift Tasks

1. A police officer enters his 10-hour shift at the Brookside jurisdiction. After completing his administrative check-in, the officer takes his duty equipment to the squad car assigned to him for the shift. In the vehicle, the officer initiates his biometric identity check with his PSCD. After authenticating the officer, the system sets up a profile of the officer on the PSCD and the network, establishes the level of data access the officer is authorized to have across available databases, and initiates tracking of the officer's activities. The officer initiates the equipment self tests of the devices he will be using within the vehicle. The data terminals, status monitors, video cameras, displays, three-dimensional location sensor, etc., are integrated into a PAN. All of the devices code their information with the officer's ID, conduct their registration/authorization steps, and report their status to the wireless network. Each device will be associated with the officer and will provide that officer with capabilities based on the officer's profile. When the officer starts the vehicle, the JAN recognizes the officer's PSCD and uploads the pertinent database files, the latest law enforcement alerts, and the current road and weather conditions to the PSCD.

2. After successfully completing all the self tests, and receiving all the updates from the JAN, the officer provides a digital status to the network indicating that he has completed all initial setups and is ready. The Police Center network reports to the dispatcher, via the center's data systems and on-vehicle data systems, identifying which personnel and equipment are active and available for calls. The officer follows up with a PSCD voice call with the same message. The dispatcher acknowledges that the officer is active and that dispatch's GIS and CAD systems are properly receiving location and status data from the officer's vehicle and monitor units.

3.4.2 Law Enforcement Response to a Traffic Stop

1. While on routine traffic patrol, the officer observes a car that runs through a red light at an intersection. The officer presses the “Vehicle Stop” button on his vehicle's PSCD. The PSCD issues a message to dispatch, noting the operation underway, the officer's ID, and the location information of the officer's car. As the officer drives his squad car, the license number of the offending vehicle is captured by license plate recognition software and sent back for a query to the Department of Motor Vehicles (DMV). The video camera on the officer's vehicle dashboard begins recording video of the offending vehicle to a device in the officer’s vehicle. This video can be accessed at any time, on-demand, by the dispatcher and other authorized viewers. Other units in the area are alerted to the impending vehicle stop.

2. Shortly, the State Motor Vehicle Registration, Stolen Vehicle, and Wants/Warrants systems return their information to the vehicle’s PSCD. The officer also receives a picture of and information about the registered owner; the information indicates, both on the PSCD screen and with an audio signal, that there are no wants/warrants.

3. The offending vehicle pulls over and stops. The video feed will be available to dispatchers and supervisors on demand, or automatically displayed in the case of an emergency. When the officer leaves his squad car, he has access to all of his communications and data devices as the devices continue to communicate between his PAN and the vehicle's IAN node. The officer approaches the car and notes that there is a single occupant, the driver. The officer requests the driver's license and registration, but the driver does not provide documentation.

4. While requesting the information from the driver, the officer observes what he believes to be the remains of marijuana cigarettes in the ashtray. The officer decides to search the suspect's vehicle and contacts dispatch to request a backup unit. The dispatcher enters the “Dispatch Backup” command for the incident on the dispatch terminal, and the CAD system recommends the dispatch of the closest unit based on automatic vehicle location (AVL) information provided by the vehicles on patrol and known road and traffic conditions. The dispatcher glances at the console map to confirm the recommendation and presses the key to confirm the CAD recommendation. The dispatch of the backup unit is transmitted electronically to terminals in that vehicle, as well as to other nearby units and the area supervisor's car for informational purposes. A temporary PSCUG is created between the original and backup officer to share information, both voice and data. The backup officer acknowledges dispatch and asks the on-scene officer to confirm location and circumstances.

5. The supervisor and backup officer bring up the real-time video of the event in their vehicles and briefly observe the situation. All appears under control, and they release the video link. The backup unit arrives on scene. The responding officer orders the suspect to get out of his car. The backup officer watches the driver while the original officer searches the car. The original officer finds a number of bags of a white substance that appears to be cocaine. The original officer then places the driver under arrest and restrains him with handcuffs. The officer also attaches a bracelet equipped with an RFID tag to the driver. The RFID tag is then loaded with the officer's identity code, the nature of the crime, and a case number via the PSCD. The original officer radios dispatch to request a transport vehicle. The transport unit is dispatched and is added to the PSCUG, with the original officer to communicate and obtain information as needed.

6. After the arrest, the officer takes the driver's biometric sample with his PSCD. The PSCD submits the scan data to the biometric ID database for identification. Soon after, the PSCD returns an image, name, date of birth, and physical characteristics of the individual from the biometric sample that matches the name and date of birth of one of the aliases returned by the license plate check, and matches the driver's license picture. This indicates that the driver is the registered

owner of the vehicle. The officer queries the criminal history database for information about the driver and receives a response that the individual has previously been arrested for drug possession.

7. When the transport unit arrives on scene, its vehicle is automatically linked with the original PSCUG. The transport unit takes control of the arrested driver and transports him to the jail. The backup unit departs the scene and resumes patrol. The transport unit is removed from the PSCUG.

8. The officer takes photographic images of the suspect's car and the suspected drugs and collects the evidence. He conducts field tests of the substances and confirms that the suspected drugs are cocaine. He places RFID tags on all the evidence bags.

9. The officer radios dispatch to request a tow truck to impound the vehicle. Dispatch notifies the tow company, and the officer communicates directly with the tow truck operator to confirm location and status. While waiting for the tow truck, the officer completes preliminary suspect and vehicle information on the crime to automatically populate the electronic Tow Report and Inventory Form and the Jail Booking Form. All of the data is cross-referenced in each report so that the officer needs to fill in each type of information only once. This information is transmitted to the Sheriff's Central Records System.

10. The transport officers arrive at the jail located in Central City. The officers bring the suspect in for booking. The booking officer queries the suspect's RFID tag on the bracelet to begin the booking record, which is automatically populated from the information previously sent to the Central Records System. Information on the RFID tag is cloned to a wristband that is then affixed to the suspect after the handcuffs and the bracelet are removed.

11. As the tow truck arrives, the truck is added to the IAN at the scene. The tow truck and driver are registered and authorized to exchange information on the network. The tow truck company information automatically populates the Tow Report. The tow truck driver reviews the Tow Report with the associated officer code and case number, and adds his electronic signature.

    The officer then continues to work on the arrest report, adding a vocal narrative section describing the events, along with descriptions of the confiscated property and associated arrest information. The officer also updates the State Motor Vehicle database to show the vehicle status as “towed/stored.”

12. The officer completes the arrest report in electronic form. The report is transmitted to the officer's supervisor. The supervisor notes one deficiency in the report and issues it back to the officer. The officer corrects the report and retransmits it to the supervisor, who electronically signs off on the report, and forwards it to the Central Records System and to the District Attorney's office.

13. The officer clears the incident on his PSCD, which automatically shuts off the video camera and resumes patrol.

3.4.3 Law Enforcement Communications Summary

Throughout the scenario, the network tracks the law enforcement personnel and equipment, as well as the arrested suspect, and provides geolocation information in real time to supply the field supervisor as well as dispatch with the current accountability of all personnel. All suspect information and evidence are recorded through wireless monitors and voice recognition systems, with no reliance on paper reports and notes. All information is tagged with the original officer's identity code. All evidence is tracked with RFIDs to provide an audit trail. All law enforcement personnel and equipment have monitors to measure vital conditions and status that are reported by the PSCD and IAN to the IC's management system.

National and state criminal justice records and state civilian records are searched and queried for information relating to the traffic stop, as well as other data.

3.5 Multi-Discipline/Multi-Jurisdiction-Explosion Scenario

This scenario focuses on the command and control, asset status and tracking, and major communications interoperability aspects of an incident involving first responders. The scenario occurs from the perspective of the IC and Emergency Manager (EM), and does not include first person, first responder perspectives. The communications capabilities described in the three first responder scenarios are implied (but not described) in this scenario. The italicized text indicates actions or responses of the EM.

3.5.1 Explosion

1. A large explosion occurs at a chemical plant in Barberville, a suburb of Brookside. A potential exists for hazardous chemical leaks as well as toxic smoke from the burning chemicals.
2. IC arrives on scene and assesses the situation. After briefly surveying the area, the IC team initiates its mobile command center and begins to receive information from the temporary network created by the on-site first responder vehicles and personnel.
3. *The EM is alerted that a major incident has occurred and brings up the command terminal in the Emergency Operations Center (EOC) to monitor the regional situation. All of the region's assets are available for query by the EM.*
4. The mobile command center's display registers all of the assets that are currently on scene, including EMS, Law Enforcement (LE), and fire. The status of each asset is also available, but is displayed on demand.
5. IC shifts the display to a GIS overlay of the explosion, with the location of all assets shown. Areas are marked to display casualties, fires, evidence, the incident perimeter, etc. The information for the GIS displays comes from a site survey already underway by LE, fire, and EMS personnel.
6. *Information is available on the EM's system as the information is gathered by IC. This information is shown both in a GIS map format as well as a textual set of data. On demand, the EM can call up the information on the incident as though the EM were on site in the capacity of IC.*
7. As new units arrive on scene, they are authenticated into the incident and added to the list of assets available to IC.
8. The on-scene Fire Branch monitors the status, location, and current duties of the fire assets on its command screen, and reassigns those assets as necessary. Any data that is pertinent to the other branches and IC is automatically forwarded to their command systems. This same situation is repeated for the LE Branch as well as the EMS Branch.
9. After completing all of the pre-defined tasks for this particular type of incident, IC begins coordinating with the LE, EMS, and fire command posts. As IC begins directing the assets in the field, the Fire Branch informs IC that the incident is too large to be handled by the assets on hand. IC then puts in a request to the EM for the acquisition of more fire units.
10. *As the request for more fire assets comes into the EM, the EM initiates the mutual-aid agreements in place, and units are dispatched from the Brookside metropolitan area to Barberville.*

11. The EMS Branch sets up a triage/treatment area, and begins to direct the resources available to identify and handle casualties. The location of the triage/treatment area is disseminated to all first responders on scene, and its status is made aware to area medical facilities.

12. The Fire Branch is notified of an emergency on its command screen as one of the firefighters in the field has a passive sensor triggered by the detection of a hazardous chemical. The sensor determines that the hazardous chemical would not be ignited by a radio transmission, allowing the network to notify all first responders within 100 feet of that particular firefighter along with LE, EMS, and IC. The Fire Branch designates this area as a Hot Zone, which alerts any personnel entering the designated area to its status.

13. *Because of the potential for the release of hazardous chemicals, the EM directs all available hazardous materials (Hazmat) teams to the location and puts these assets under the control of IC.*

14. IC sets up a secondary perimeter five blocks back from the incident.

15. *The EM notes the perimeter change, and starts the process for a reverse 911 warning call that is sent to all fixed and cellular telephones inside the secondary perimeter. This call instructs the people inside the perimeter to find shelter in the area quickly and to close off all outside ventilation.*

16. The LE Branch is directed by IC to coordinate with the Department of Transportation to configure traffic management assets, such as traffic lights and electronic signs, to divert traffic away from the incident.

17. The LE Branch has enough assets to establish a perimeter but needs more assets to maintain the security of the incident. IC puts in a request for LE assets to the EM.

18. *The EM begins to coordinate with the public utilities and other pertinent private organizations for the appropriate responses, such as shutting down gas lines to the area and dispatching electrical crews to handle situations, such as downed power lines. The EM also directs additional LE assets into the area upon receiving the request from IC.*

19. Upon further investigation by LE and fire assets, IC determines that this explosion was not an accident, directs LE to treat the area as a crime scene, and assigns detectives to begin an investigation of the crime scene in coordination with fire investigators. This information is also available to the EM.

20. After determining that the probable cause of the situation is a bomb, IC directs the LE Branch to begin directing traffic away from the scene, and to initiate a secondary explosive device search by the Explosive Ordinance Disposal (EOD) team.

21. The EMS Branch continues to coordinate the efforts of EMS assets. As casualty information comes onto the command screen via the RFID tags used by personnel in the field, the most critical cases are selected for transport to the nearest available hospitals. The EMS Branch believes that the on-scene casualties will overburden the medical facilities selected to handle them. The transportation officer is directed to query the local medical facilities regarding their status, capacity for casualties, and what types of casualties can be taken. Casualty statistics are available on demand by IC and the EM. Additionally, the local medical centers coordinate among themselves on resource availability.

22. *The EM begins to monitor the status of the casualties, as well as the status of the responding medical facilities. Recognizing the casualties from the incident will overburden the nearby facilities, the EM puts a neighboring medical facility on alert for incoming casualties. The EM also directs additional EMS crews to respond to the incident.*

23. As EMS assets arrive on scene, the assets are registered, and their capabilities are authorized for placement into the EMS asset pool for assignments given by the EMS Branch.

24. The Unit Commander of the EOD team notifies the LE Branch that no secondary devices have been found. The LE Branch pushes this information to IC. IC automatically forwards this information to the EM.

25. The Fire Branch alerts IC that all of the fires have been identified and are marginally contained. Additionally, the hazardous chemical spill has been contained and eliminated by the Hazmat teams dispatched by the EM. All but one Hazmat team is released back into the regional asset pool.

26. The Fire Branch alerts IC that all of the fires have been eliminated, and that all but one fire crew has been released back into the regional asset pool.

27. The EMS Branch alerts IC that all of the casualties have been evacuated to appropriate medical facilities. The coroner has been contacted to begin removal of the deceased.

3.5.2 Multi-Discipline/Multi-Jurisdiction Communications Summary

The abstracted view of ICs is very different from that of a first responder reacting to a situation in the field. Consequently, their communications needs and capabilities are tailored to meet those differences. While the communications and actions depicted in the scenario are oversimplified versions of what would actually have occurred, what has been captured is the general nature of the communications, the command and control functionality, and examples of access to a wide variety of information on an on-demand basis.

The command and control of IC on scene and the EM provide for the safety and accountability of all the assets at the incident, and supply information on additional resources that could be brought to the incident. The networks for communications and information exchange are created on an ad hoc or temporary basis at the scenes. They overlay on one another to provide interoperability and integrate with the larger JANs to form a system of systems for command and control.

This page intentionally left blank.

4 Operational Requirements of PS C&I

Multiple levels of interaction occur among public safety disciplines and jurisdictions. This section defines the levels of intra-agency "operability" and interagency "interoperability" that occur for each major public safety discipline.

Public safety communications are defined in the area of operability, and the following three areas of interoperability based on their internal and external interactions:

- Day-to-Day
- Task Force
- Mutual Aid

This PS SoR document focuses on interoperability of communications, but it also recognizes that public safety agencies must first have operability before they will be able to address interoperability. The PSWAC Final Report[3] defined three modes of communications, but this PS SoR will treat some of these modes differently than either the PSWAC Final Report or what is common public safety usage for the terms, outlined as follows:

- Users estimate 90 percent of all public safety land mobile radio (LMR) usage is for day-to-day situations. Day-to-day interoperability requirements surface when a city police officer must communicate with a county sheriff deputy, for example, and interoperable wireless communications are a requirement. Another example might be a public safety response to a life-threatening traffic accident in which first responders of Fire, Law Enforcement, and EMS respond and require the ability to intercommunicate.
- The task force category refers to the operations of multiple public safety agencies working on a focused activity, such as a Drug Task Force in which the wireless communications must be highly coordinated and interoperable. The other distinct form of task force is used by a single agency to define a particular effort, such as a fire regulations task force in which other agencies are not involved in the effort and interoperable communications are not required.
- The mutual aid category addresses mutual-aid pact and emergency management assistance compact relationships agreed to by city mayors, county commissioners or supervisors, or state governors. These provide additional coordinated resources for joint combat of emergencies or disasters. Joint response requires wireless interoperability to support coordinated resources.

The following subsections first define the operations of public safety agencies with general requirements associated with those operations and, second, describe specific operations for each of the first responder groups with their specific communications requirements. All of these services are provided by first responders at the local, tribal, county, and state levels. The Federal Government has few first responder organizations, with those primarily providing such services on large Federal properties, such as national forests and parks and on military bases.

3. Irving, Larry, *Final Report of the Public Safety Wireless Advisory Committee (PSWAC) to the Federal Communications Commission and the National Telecommunications and Information Administration*, September 11, 1996.

4.1 Public Safety Operations Background

4.1.1 Disciplines

Previous sections of the PS SoR have referred to public safety agencies and the supplemental agencies that provide support, such as departments of transportation, or related agencies that provide complementary functions, such as judicial systems. In this section, the discussion concentrates on the public safety first responders, namely:

- Structure Fire and Wildfire Suppression Services
- EMS. The components of the EMS system include the following:
  - Medical first responders (people and agencies that provide non-transporting first aid care before an ambulance arrives on scene)
  - Ambulance services (basic and advanced life support, etc.)
  - Specialty transport services (helicopter, boat, snowmobile, etc.)
  - Hospitals (emergency, intensive, cardiac, neonatal care units, etc.)
  - Specialty centers (trauma, burn, cardiac, drug units, etc.)

  This section refers to out-of-hospital EMS personnel, including paramedics and emergency medical technicians (EMT) who are on scene at the incident.
- Law Enforcement Services

The PS SoR concentrates on first responders' operational needs for communications because their requirements exceed those of all other agencies for most performance values, such as ease of operation, reliability, restorability, scalability, availability, harsh environment operation ability, etc.

4.1.2 Jurisdictions

As noted earlier, public safety first responders are either found in all jurisdictions or operate with others in all jurisdictions, namely:

- Local/County/Regional
- State
- Tribal
- Federal

Public safety agencies interact with one another by discipline as well as by jurisdictions. Communications systems must be able to cut across all levels of interaction just as the practitioners of the agencies cut across all levels.

4.1.3 Hierarchy and Modes of Operations

The hierarchy levels of communications include:

a. Intra-agency:
   - Single Discipline/Single Jurisdiction

b. Interagency:

- Single Discipline/Multiple Jurisdictions
- Multiple Disciplines/Single Jurisdiction
- Multiple Disciplines/Multiple Jurisdictions

The hierarchical levels define increasingly complex communications interactions and administration as the hierarchy moves from the single discipline/single jurisdiction situation to the multiple disciplines/multiple jurisdictions events. The level or hierarchy of the communications operations interaction should not cause confusion and frustration for the first responder. The first responder must be able to respond and react to each level without regard to the communications requirements and the communications functionality must be invisible to the first responder. Additionally, the first responder must be able to move seamlessly and transparently from jurisdiction to jurisdiction with no interruption in service, provided the user is authorized as local policy dictates.

There are many modes of public safety operations and an equal number of ways to classify them. The PSWAC Final Report defined the interagency modes based on the needs for "communications interoperability" according to characteristics that clearly define each of the three modes. In the next sections, the PSWAC modes are identified as well as agency internal modes common to public safety.

4.1.3.1 Modes of Routine Intra-Agency Operability:

1. Normal operations within a discipline
2. Communications that are rehearsed and practiced every day
3. Day-to-day patrols and duties, and responses to dispatches from emergency call centers
4. Task force operations within a discipline or agency for a specific mission

4.1.3.2 Modes of Interagency Interoperability:

1. Day-to-Day:
   - Communications that are rehearsed and practiced every day
   - Routine operations with neighboring agencies to provide support or backup
   - It is estimated that this form of interoperability makes up 90 percent of an individual first responder's multi-agency activities
2. Task Force:
   - Cooperative effort among mixed yet specific agencies and disciplines
   - Extensive pre-planning with practice
   - Operations that are planned or scheduled and are proactive
   - Operations that have a common goal, common leader, and common communications
3. Mutual Aid:
   - Major event that causes a large number of agencies to respond and requires considerable coordination
   - Major event that requires response from multiple jurisdictions from the local level to the state and national level

- Communications that operate under a state or regional mutual-aid pact
- Operations that are usually not planned or rehearsed, but which react to the situation

4.1.3.3 Overlap and Modes

Although there is much overlap of the modes of operation, it is useful to divide the discussion among the four modes. The operability and day-to-day interoperability modes fit a general normal structure for public safety personnel, and should not tax their ability to deal with communications processes and procedures. Many of these operations may be strictly within the discipline or agency, with no communications interoperability requirements with other disciplines or agencies at all. However, as described in the PSWAC Final Report, day-to-day operations can routinely include the need for local LE personnel to communicate with county LE personnel, and vice versa. This ability to communicate minimizes the need for dispatcher-to-dispatcher interaction in the exchange of information among units in the field. Day-to-day operations can also include intra-agency task force operations to carry out a specific mission, such as a DUI (Driving Under the Influence) checkpoint, in which the communications are within the agency and do not require interoperability with other agencies. Also on a day-to-day basis, an agency, such as one fire district, can routinely back up another, while another agency covers an emergency.

The task force mode defines a cooperative effort between specific agencies with extensive pre-planning and practice of the operation. As the PSWAC Final Report indicates, the communications tend to be at close range, and the traffic requires rapid or immediate response times. In today's environment, task forces, such as a terrorism task force, may cover a broad regional area and not operate exclusively at close range. These operations present additional challenges.

The mutual aid mode describes major events with large numbers of agencies involved, including agencies from remote locations. Their communications are not usually well planned or rehearsed. The communications must allow the individual agencies to carry out their missions at the event, but follow the command and control structure appropriate to coordinate the many agencies involved with the event.

While the PSWAC Final Report defined these modes of operation to stress the need for communications interoperability among the first responders, the majority (as much as 90 percent) of the communications usage falls under the day-to-day operations mode. Thus, the communications systems must support the day-to-day operations with all the same performance features that may be required to support the other modes of operation. Unless the systems provide the first responders with seamless functionality regardless of the mode of operation, the first responders will not use their systems efficiently or effectively, especially when they need to operate in the task force and mutual aid modes.

4.1.4 Security

In much of the following discussion, the need for security in communications and information sharing is implied.

As a general rule, the principles of security for public safety communications and information sharing include the following requirements:

1. Access Control and Authorization

   Both the public safety users as well as the public safety user's device(s) must be authenticated before they are given access to network resources, and the communication networks must ensure users do not exceed their allowed authorities.

2. Data Integrity

The communication networks must not allow unauthorized interception/modification of communications or information, they must not allow communications replay attacks, and they must have non-repudiation capabilities to ensure availability of evidence in the event of a dispute.

3. Privacy

   The communications systems must allow only intended and authorized recipients to hear/see/read information as well as adhere to national and state policies (e.g., HIPAA).

4. Attack Prevention and Detection

   The communications networks must be resistant to jamming, they must be capable of passive/active attack monitoring and defense deployment, they must be able to geolocate the source of an attack, and they must be capable of monitoring of all functional aspects by authorized users/devices.

5. Physical Security

   In addition to protecting communications as it is occurring across a system of systems, specific attention must also be paid to the physical security of the components that make up the system. Access to infrastructure sites and mobile/portable PSCDs must be limited to authorized individuals.

Although security is identified as a separate topic for discussion, it must be fully integrated in the development and implementation of the communications systems. Security cannot be added on after the fact or as a last resort.

4.1.5 Command and Control

Public safety operations follow a command and control hierarchy that allows public safety personnel to work seamlessly on situations that may begin small, but can evolve into large incidents requiring many resources and assistance from numerous jurisdictions. As an incident grows in magnitude, the IC has to know what resources and capabilities are becoming available for use. Each of the first responder disciplines may have its own branch commander at a large incident, and these branch commanders must be able to coordinate, communicate, and share information with the overall IC.

The communications systems that support these operations must also be capable of the same command and control features, as follows:

1. Incident Command System (ICS)[4]

   The communications systems must support the agency's incident command policies.

2. System administration of users

   The communications systems must allow authorized system administrators, as well as incident and branch commanders, to establish user profiles for network access and usage, depending upon the role that the public safety user is asked to satisfy during an incident.

3. User identification and location

4. NIMS Basic "The Incident Command System," FEMA 501-8, March 27, 2006, Revision 0. http://www.fema.gov/pdf/nims/NIMS_basic_incident_command_system.pdf. (cited August 2006)

The communications systems must provide user identification to others during communications and, when required, must provide user geolocation information to ICs and other authorized resources.

In addition, the system must allow communications and information sharing between IC or unified command operations with an EOC. In some instances, the EOC requires on-demand access to GIS-based displays, video, and communications as they are occurring at the incident.

4.1.6 Communications Needs for Public Safety Operations

The next subsections describe the activities of public safety agencies in various activities, e.g. wildfire suppression or EMS, and how wireless communications and information resources are needed to support those activities. These sections are somewhat similar to the scenario section, but further identify how communications and information will be used by the first responders during intra- and inter-jurisdictional operations.

The modes of communications are divided into four categories.

- Voice communications—Interactive.
- Voice communications—Non-interactive.
- Data communications—Interactive.
- Data communications—Non-interactive.

For each of the modes of operational communication and for each of the categories of public safety first responders, next the following subsections describe the operational uses of communications and information in the context of the following parameters:

- With whom
- For what purpose
- With what special constraints, i.e., considerations, needs, and requirements (e.g., time limits, encryption, access to sensitive information, etc.)

In the following discussions, all intra- or inter-agency communications and information sharing are assumed to be allowed only when the users are authorized by their agencies.

4.2 Structure Fire and Wildfire Suppression Services

4.2.1 Routine Operability and Day-to-Day Interoperability

These activities are centered on response to building fires and wildfires; specialty fires, such as at airports; search and rescue missions; emergency calls (911); traffic accidents; water recreation accidents; Hazmat incidents; medical emergencies; and other emergency events. In larger cities, fire suppression services are provided by full-time municipal government employees, who also may provide emergency medical assistance and other related services. In other more rural settings, fire suppression services are often provided by organized and trained volunteers. States have divisions of natural resources or state forestry departments with teams experienced in fighting wildfires within the state. Federal land management agencies, such as the Department of the Interior's National Park Service and Bureau of Land Management or the Department of Agriculture's Forest Service, have wildfire suppression programs and personnel.

The majority of fire operations are within the routine operability and day-to-day interoperability categories. Fire departments (FDs) often use interoperability on a day-to-day basis. For example, when a particular fire station responds to a structure fire, a neighboring fire station essentially increases its response area by covering for the first fire station that is responding to the structure fire, maintaining interoperability with the first station.

4.2.2 Task Force

Routine fire suppression scenarios often meet the definition of task force operations. For sporting events and other large public gatherings that can be planned in advance, fire response teams will be coordinated. They may stage equipment and other resources at the event that are needed to communicate with a local command post. This mode assumes the same operational needs as day-to-day operations, although the needs may need to be expanded in scope for the larger events entailed.

4.2.3 Mutual Aid

Mutual aid for the fire services can occur in a wide range of situations, including extreme weather conditions, such as hurricanes, flooding, and tornadoes; earthquakes; major explosions (terrorist or accidental); plane crashes; major fires; riots. These large-scale disasters are not planned. Disasters stress communications capabilities the most and are discussed in the following sections.

Mutual aid operations are characterized by a large number of neighboring agencies, personnel, and equipment brought in to assist the affected jurisdiction. These include agencies from neighboring regions, neighboring states, Federal agencies, and occasionally agencies from outside of the United States. Communications with all of these additional personnel and a temporary command structure will be required, via existing infrastructure (if still operational) and extra temporary infrastructure brought in for the duration of the emergency. Contacts may include LE, traffic control, fire response, EMS, utilities, public works, transportation, Hazmat units, urban search and rescue, military, National Guard, relief agencies, weather information, temporary housing and food organizations, and volunteers, depending on the scale and type of the event.

The mutual aid communications functions needed for firefighting are similar in nature to everyday operations, except for the greatly increased scale of the effort and for the shortages of equipment, personnel, and water that are common. In large-scale disasters, there is often greater uncertainty about the location and condition of victims, while responders must at the same time contend with such situations as multiple fires, water shortages, rescue operations, police actions, overloaded communications and transportation resources, and other serious and dangerous distractions that accompany these events.

During these events, firefighting operations must continue at a high level of efficiency, with intensive dependence on large numbers of extra workers from neighboring agencies and jurisdictions.

Also falling into the category of mutual aid are extremely large planned events, such as political conventions, the Olympics, and international meetings in which a host state's mutual aid pact is activated in advance. In such events, as with smaller task-force-based events, fire suppression response will be coordinated. It is anticipated that large amounts of resources will be staged nearby to support these events, including resources to deal with potential disruption and civil unrest that might occur around the event. The public will expect the provision of day-to-day level services throughout the event while the host agency continues to provide the same level of services to the remainder of its jurisdiction.

4.2.4 Voice Communications—Interactive

Table 4: Fire Voice Communication—Interactive

The communication occurs:	
with whom	Public Safety Answering Point (PSAP) such as a 911 call center; public safety communication center; supervising officers and ICs; other firefighters at scene; police and other emergency workers on selected user groups; selected user groups in neighboring areas; agencies to control traffic and crowds, and to coordinate with local hospitals, emergency rooms, and doctors. Dispatcher and supervising officers, IC officers and other participants, or any other persons on a person-to-person basis, including the Public Switched Telephone Network (PSTN) when authorized.
for what purpose	These voice calls are to receive instructions from the dispatcher and to coordinate with the IC; coordinate efforts with local and neighboring FDs or natural resource management agencies for additional assistance and equipment; coordinate with local and neighboring police and other agencies for traffic and crowd control; gain information on building ownership/contents/personnel; obtain detailed medical advice on treatment of victims and instructions for transportation, etc.
with what special constraints	Many of these calls are very high-priority, are mission-critical, and may need to be secured to protect privacy and maintain chain-of-command authority.

4.2.5 Voice Communications—Non-Interactive

Table 5: Fire Voice Communication—Non-Interactive

The communication occurs:	
with whom	Dispatchers, via voice pagers, or other fire officials in local and neighboring agencies using paging receivers. ICs and supervisors via PSCDs.
for what purpose	Voice paging is used to alert volunteer fire personnel concerning an immediate need for their services. Voice calls transmit instructions from the dispatcher and to coordinate with the IC.
with what special constraints	Many of these calls are very high-priority, and need to be secured to protect privacy and maintain chain-of-command authority.

4.2.6 Data Communications—Interactive

4.2.6.1 Accountability Communications

Table 6: Fire Data Communication—Interactive 1

The communication occurs:	
with whom	Other firefighters. To share a unique responsibility for each other and for those under their command to provide immediate aid relative to a firefighting activity.
for what purpose	These communications are for firefighter safety and accountability. The goal is to know where every firefighter is located, to know the firefighter's health and condition, and to have the ability to remove the firefighter from life-threatening situations. Also, all firefighting equipment needs to be located and tracked through an AVL system. The data must be continuously updated on the IC's GIS and the dispatcher's CAD displays to indicate the location and health of all firefighter assets, as well as pre-planning information and Hazmat locations.
with what special constraints	This data must be current, accurate, time-sensitive, and have a high priority. The data would include the firefighter's three-dimensional location with high resolution; the firefighter's biometrics, such as heart rate, temperature, respiratory rate, and blood pressure; and the firefighter's equipment status, such as the level of oxygen remaining in an oxygen tank. The data must be able to be used to notify nearby firefighters of the location of the firefighter seeking aid and to “vector” the rescuing firefighter to the firefighter requiring aid.

4.2.6.2 Text Messages

Table 7: Fire Data Communication—Interactive 2

The communication occurs:	
with whom	Exchange information among firefighters and others via interactive messaging. Exchange information with systems that may include data repositories, databases, and active files on a wide range of public safety activities from local and neighboring jurisdictions and agencies. These exchanges will require immediate responses from other individuals or data systems.
for what purpose	Text data communications is used for access to current and archived computerized information, e.g., information about contents, uses, ownership of buildings; medical records of patients; and for printing backup of incident-related communications sent earlier via a voice call, etc. In addition, data communications are used to file reports remotely and electronically (using office-in-a-vehicle capabilities), so that they are rapidly available to local and neighboring public safety officials.

Table 7: Fire Data Communication—Interactive 2 (Continued)

The communication occurs:	
with what special constraints	Much of this data is very high-priority, and needs to be secured to protect privacy and maintain chain-of-command authority.

4.2.6.3 Image Communications

Table 8: Fire Data Communication—Interactive 3

The communication occurs:	
with whom	Communicate with local, state, and national databases, various local and neighboring public safety personnel working on the incident, dispatchers, and command officers. Databases include archived maps, photographs, building drawings, etc. and active files on a wide range of public safety activities from local and neighboring jurisdictions and agencies.
for what purpose	The images are transferred for a wide range of purposes to assist firefighters on the scene or to aid the ICs with visual information. Maps and drawings of buildings, roads, utilities, hazardous locations, hydrants, and terrain serve a wide range of planning, firefighting, traffic control, and search functions. Current pictures taken at a fire scene (ground level and aerial) are useful immediately for tactical firefighting decisions. Pictures of victims are needed to help doctors at distant sites recommend the best medical response to injuries.
with what special constraints	These communications require rapid response and thus are considered interactive. These images are high-priority and require rapid transmission. Encryption will be needed to preserve privacy and prevent the release of critical data.

4.2.6.4 Video Communications

Table 9: Fire Data Communication—Interactive 4

The communication occurs:	
with whom	To send video images between fire personnel in the field, remote dispatchers or ICs, and medical doctors. Video images are also used to control robotic devices to observe inside burning buildings, collapsed structures, underwater rescues and recoveries, etc. Some of these images are also likely to originate from aerial video coverage.

Table 9: Fire Data Communication—Interactive 4 (Continued)

The communication occurs:	
for what purpose	Ground-based and aerial video pictures taken at the scene of a fire or other emergency sites are extremely useful for immediate tactical firefighting responses, to coordinate rescue efforts, to help distant medical personnel evaluate patient condition and treatment, etc. These video pictures can also include specialized non-visual imaging to warn of spreading fire, chemical hazards, etc. Robotics video is needed at the site to aid in controlling robotics devices, but is also useful for tactical direction by the incident commander.
with what special constraints	Real-time video is extremely valuable in numerous firefighting and medical situations, both locally and remotely, even though it may require substantial resources to transport it from the scene to observers. Many situations will require very high resolution to provide the observer clear video pictures. Some of this video should be encrypted.

4.2.7 Data Communications—Non-Interactive

4.2.7.1 Text Messages

Table 10: Fire Data Communication—Non-interactive 1

The communication occurs:	
with whom	Communicate with local and neighboring agencies using e-mail connections, Web browsers, etc. Send to the FD command post each firefighter's personal biometrics (heart rate, breathing rate, body temperature, etc.) from the fire scene, resources status (oxygen tank, water pressure, battery capacity, etc.), and physical location. Send large equipment resource status (tanker water pressure, location, etc.) to the FD command post. Send warning pages to indicate hazardous conditions.
for what purpose	The fire-scene personnel and equipment status allow the FD command post to track and control all resources, provides fire personnel with real-time traffic status (such as, Intelligent Transportation System (ITS) information) for traffic congestion updates, and provides drivers with the capability to control traffic lights during an emergency.
with what special constraints	Much of this data is very-high-priority. The data would be polled from the field units, or the field units would need to “push” the information to the command post about every second from personnel and about every 30 seconds from large equipment resources.

4.2.7.2 Image Communications

Table 11: Fire Data Communication—Non-Interactive 2

The communication occurs:	
with whom	Communicate with the incident command post. At the fire scene, head-mounted IR cameras on the firefighters send images to the FD command post. Firefighters also receive images from the command post.
for what purpose	The images are transferred for a wide range of purposes to assist firefighters on the scene or to aid the ICs with visual information. IR images allow the FD command post to track the development and suppression of the fires by mapping the IR hot spots. Maps and drawings of buildings with room locations, as presented on a firefighter's heads-up display, assist in fire suppression and search-and-rescue functions.
with what special constraints	These images are high-priority and require rapid transmission.

4.2.7.3 Video Communications

Table 12: Fire Data Communication—Non-Interactive 3

The communication occurs:	
with whom	Send video images from fixed locations in the field to ICs.
for what purpose	Ground-based and aerial video pictures taken at the scene of a fire or other emergency sites are used to monitor situations without requiring fire personnel to be on-scene observers. By using video as well as IR images, weather data, wind speed, etc., all chained to a GIS application, the IC is given a highly useful tool to predict fire behavior and progress.
with what special constraints	Usually, high-resolution video images are not needed for monitoring.

4.3 Emergency Medical Services

4.3.1 Routine Operability and Day-to-Day Interoperability

These activities are centered on response to emergency calls (911) for medical emergencies, traffic accidents, water recreation accidents, building fires, Hazmat incidents, and other events. Although the services provided are similar in various areas, the administrative arrangements to provide these services may differ substantially. In many cities, EMS is provided as part of municipal government, often as part of the EMS/FD activities. In other cities, private ambulance companies, hospital-based ambulance services, volunteer EMT-ambulance services (making up as much as 60 percent of some states' providers), and other agencies perform more of the EMS functions.

The basic services include patient stabilization from medical emergencies, such as cardiac and respiratory events, and motor vehicle and other trauma, often in concert with extrication by fire and/or search and rescue teams. It also usually includes transport of the victim or patient to more intensive care in hospital/ER facilities or to medical specialty centers (trauma, burn, cardiac, etc.) Mutual aid operations occur daily when one hospital accepts emergency patients diverted from another hospital for EMS.

These day-to-day incidents, along with emergency and non-emergency transports among facilities, form the bulk of the operations performed by EMS personnel. An expanded future role for EMS[5] may include more requirements for assistance to physicians and hospitals with routine patient care; these additional operations may affect communications.

4.3.2 Task Force

EMS scenarios usually consist of a series of high-priority incidents involving task force operations working with other first responder agencies. For sporting events and other large public gatherings that can be planned in advance, EMS teams will be coordinated. They may have an emergency clinic at the event, and the clinic may need to communicate with hospitals and ambulances. This section assumes the same operational needs as day-to-day operations, although they may need to be expanded in scope or targeted to specific areas for these larger events.

4.3.3 Mutual Aid

Mutual aid for EMS can occur in a wide range of situations, including extreme weather conditions, such as hurricanes, flooding, and tornadoes; earthquakes; major explosions (terrorist or accidental); multi-vehicle car crashes; plane crashes; major fires; and riots.

These large-scale disaster events are not planned. Disaster events are those that stress communications capabilities the most and are discussed in the next sections. Also falling into the category of mutual aid are extremely large planned events, such as political conventions, the Olympics, and international meetings in which a host state's mutual aid pact is activated in advance. In such events, as with smaller task-force-based events, EMS teams will be coordinated. There will be emergency clinics at the event, and these clinics will need to communicate with hospitals and ambulances. It is anticipated that large amounts of resources will be staged nearby to support these events, including resources to deal with potential disruption and civil unrest that might occur in conjunction with the event. The public will expect the provision of day-to-day level services throughout the event while the host agency continues to provide the same level of services to the remainder of its jurisdiction.

Mutual-aid operations are characterized by a large number of neighboring agencies, personnel, and equipment brought in to assist the affected jurisdiction. These include agencies from neighboring regions, neighboring states, and national agencies. Communications with all of these additional personnel and a temporary command structure will be required, via existing infrastructure (if still operational) and extra

5. The 1996 National Highway Traffic Safety Administration's EMS Agenda for the Future (http://www.nhtsa.dot.gov/people/injury/ems/agenda/emsman.html (Cited August 2006)) contains the following vision statement: "Emergency medical services (EMS) of the future will be community-based health management that is fully integrated with the overall health care system. It will have the ability to identify and modify illness and injury risks, provide acute illness and injury care and follow-up, and contribute to treatment of chronic conditions and community health monitoring. This new entity will be developed from redistribution of existing health care resources and will be integrated with other health care providers and public health and public safety agencies. It will improve community health and result in more appropriate use of acute health care resources. EMS will remain the public's emergency medical safety net."

temporary infrastructure brought in for the duration of the emergency. Contacts may include LE, traffic control, fire, EMS, Hazmat units, urban search and rescue, military, National Guard, relief agencies, weather information, temporary housing and food organizations, volunteers, and others, depending on the scale and type of the event. As the scale of the event increases in magnitude, the communications and control may be handed off from the local dispatcher and PSAP to a county dispatcher and EOC or to a state EOC.

The communications functions needed for EMS functions at large disasters are similar in nature to everyday EMS operations except for the greatly increased scale of the efforts. There may be a requirement to communicate with disaster medical assistance teams, or to request resources from the strategic national stockpiles for pharmaceuticals and medical supplies. In large-scale disasters, there will often be greater uncertainty about the location and identity of victims, and more intense pressure to provide adequate medical treatment with overworked treatment providers and overloaded facilities. There may be a need to transport large numbers of patients to many hospitals, including the movement of less severely injured patients to more remote hospitals or temporary facilities. There will be a need to solve immediate life-threatening medical problems while contending with fire, water, rescue operations, police actions, overloaded communications and transportation resources, and other serious and dangerous distractions that accompany these events.

During these events, EMS operations must continue at a high level of efficiency, with intensive dependence on large numbers of extra workers from neighboring agencies and jurisdictions.

Two notable exceptions to the day-to-day mode of operations will be the need to provide remote medical staging and to engage more levels of medical services, such as the county or state public health agencies.

At a large incident, the medical branch commander will need to do the following: provide staging of paramedics, EMTs, and other medical/nursing personnel, supplies, and ambulances at a site remote from the incident scene; request resources; know who is available; know the resources' estimated time of arrival (if they are not at the staging site); know their capabilities; and know what hospitals and health centers are available to receive patients.

Some large incidents deal with toxic spills, weapons of mass destruction, etc., that can affect more of the public beyond those who may be close to the incident site. In those incidents, the medical branch commander will need the ability to communicate with public health officials to help plan the evacuation of citizens, to coordinate public responses and preparations, and the like.

4.3.4 Voice Communications—Interactive

Table 13: EMS Voice—Interactive

The communication occurs:	
with whom	911 dispatchers; local hospitals, emergency rooms, and medical/nursing staff; IC officers for fires, special police operations, traffic accidents, boating and aircraft accidents; other emergency workers in selected user groups; special service providers (other specialty transportation providers, search and rescue teams, and extrication teams); traffic and crowd control personnel; and utility and public service providers. Also with dispatchers, supervising officers, selected user groups, and hospitals in neighboring areas and jurisdictions, and other individuals (such as a patient's personal physician) on a person-to-person basis via the PSTN. Talk between the cab of an ambulance (also aircraft cockpit, snowmobile, etc.) and the patient care compartment of ambulance (also aircraft patient area, snowmobile sled, etc.). Talk with life-line electronic medical emergency service providers and automatic crash notification service providers.
for what purpose	These voice calls would be used to receive instructions and assignments from the dispatcher; coordinate with the IC; inform the dispatcher of progress; ask other EMS providers or other agencies for help or information; obtain medical directions and consultations with physicians and emergency medical centers; inform receiving facilities of patient's conditions and needs; consult with supervising physicians for patient diagnosis and treatment for non-emergent conditions in which EMS provides routine community health care services; and consult with the patient's own physician. Communications can be to multiple jurisdictions, especially during the transport of patients to distant facilities. Communications could be between emergency medical dispatch personnel and patients or citizens who have called 911 to provide pre-arrival aid instructions, such as bleeding control and cardiopulmonary resuscitation, and to determine the level of EMS responders required, based on the patient's needs. Communications between the ambulance driver and the patient attendant must be via wireless headphone capability to allow hands-free operation as well as private communications between driver and attendant without the patient or the family listening to both sides of the conversation. Communications between EMS and fire rescue units for extrication, lifting patients, and locating emergency scenes. Communications between EMS and law enforcement to ensure scenes are safe for EMS personnel, to protect response crews in violent areas, etc. These communications are considered routine.

Table 13: EMS Voice—Interactive (Continued)

The communication occurs:	
with what special constraints	Many of these calls are very-high-priority. Most of these calls need to be encrypted, especially those discussions between EMS incident personnel and the hospitals or medical emergency centers. Because physicians need to know the identity of EMS incident personnel before they issue medical directions and procedures, the voice communications system needs to authenticate and authorize the personnel for the physicians, and provide the field personnel's identity to the physicians. Full-duplex with three or more people (physicians, paramedics, EMTs, etc.) with conference call-like features will be required in some cases. EMS field personnel require communications directly with hospitals and physicians and not through dispatchers. Note that these calls may need to be encrypted based on local, state, or Federal law.

4.3.5 Voice Communications—Non-Interactive

Table 14: EMS Voice Communication—Non-Interactive

The communication occurs:	
with whom	ICs, and supervisors, personnel, and system status management networks for alerts and advisories via radios; dispatch for voice paging; automated status systems.
for what purpose	These voice calls are to transmit instructions from the dispatcher and to coordinate with the IC; and for automated weather notifications, fire conditions, water, and sea states.
with what special constraints	Many of these calls are very high-priority, and need to be secured to protect privacy and maintain chain-of-command authority.

4.3.6 Data Communications—Interactive

4.3.6.1 Text Messages

Table 15: EMS Data Communication—Interactive 1

The communication occurs:	
with whom	Local and neighboring agencies, using directed text messages, and local and neighboring EMS agencies. To communicate patient medical information, telemetry, and other device-collected vital signs to and from local hospitals and emergency treatment centers. Patient vital statistics collected by EMS personnel at the incident with voice-activated recorders. Status of EMT skills, knowledge, or licensing levels and drugs/equipment and other resources onboard the ambulance for medical direction physicians (physician advisers) access to provide appropriate medical orders. Accurate location information is needed to guide EMS resources to the patient location. Also AVL information, along with vehicle and crew status, is needed by dispatchers and incident managers for closest ambulance availability. Information on assignment of patients to hospitals.
for what purpose	Text data communications are used to access current and archived computerized information; to establish the identity and medical background of patients; to communicate with responsible medical and incident personnel; to provide immediate transport of diagnostic patient medical telemetry to doctors at emergency treatment facilities and to EMS command post supervisors; and to provide EMS personnel with data on special hazards (such as toxic materials) at sites that may affect the diagnosis and treatment of patients. These communications also allow EMS personnel to collect a patient's vital statistics and to record the information using “hands-free” voice recognition data entry; for example, an EMS person's statement of “Enter patient's blood pressure of 136 over 95" would be recorded as “BP: 136/95.” Although the transmission of real-time vital statistics from an incident or from an ambulance to hospitals is not currently used or is little used by EMS personnel, the capability may be useful in the future, especially for high-risk patients. The service would need to be controlled on-command and on-demand by the hospital physicians. These communications also allow information flow between EMS field personnel and hospitals to be digitally transmitted and recorded; for example, patient information and vitals would be transmitted to the hospital and available to the physicians without needing to write the information provided, following the “enter once, use often” philosophy. Data communications also allow patient monitors to have wireless connections between the patient and the monitors, such as EKGs, stethoscopes, and blood pressure monitors, which allow for easier transport of the patient with all monitors still functioning. Additionally, local health care centers could provide access to critical medical information systems that allow EMTs to have a background on a patient. This would be on a voluntary basis and would be required to comply with security concerns.

Table 15: EMS Data Communication—Interactive 1 (Continued)

The communication occurs:	
with what special constraints	Much of this information needs to be secured to protect privacy concerns and chain-of-command for lifesaving procedures.

4.3.6.2 Image communications

Table 16: EMS Data Communication—Interactive 2

The communication occurs:	
with whom	Various public safety officials in the field, dispatchers, and command officers to access aerial photographs, pre-planned information, and local and neighboring databases. Databases include archived photographs, building drawings, road and terrain maps, etc., and active files on a wide range of public safety activities from local and neighboring jurisdictions and agencies.
for what purpose	The images are transferred for a variety of purposes, including identifying patients. Maps and drawings of buildings, roads, and geographic areas serve a wide range of planning functions, including location, rescue, and transportation of patients, traffic control, and search functions. Pictures of victims and injuries at distant sites are helpful to doctors, enabling them to recommend the best medical responses, and to law enforcement officials, enabling them to identify victims. Images of a car accident, for example, are useful to physicians in identifying the forces applied to victims within the car during the crash.
with what special constraints	These images are high-priority and require rapid transmission, and may need security.

4.3.6.3 Video Communications

Table 17: EMS Data Communication—Interactive 3

The communication occurs:	
with whom	Video images between EMS workers in the field and remote dispatchers or ICs, and medical doctors. The service is on-demand.
for what purpose	Ground-based and aerial video pictures taken at the scene of an emergency site may be useful, e.g., to help distant medical personnel evaluate patient condition and treatment. Telemedicine techniques require high-resolution video images to allow viewing such things as a patient's burns, or skin and bone details.

Table 17: EMS Data Communication—Interactive 3 (Continued)

The communication occurs:	
with what special constraints	Real-time video may be valuable for correct diagnosis and treatment in some emergency situations, but has tremendous potential for application in routine community health services, particularly in remote, rural areas where EMS personnel provide such services. The options for treatment in pre-hospital emergency settings may expand; a remote physician's viewing of the patient may become more useful. Some of this video should be encrypted. Legal requirements may not allow compression techniques, which delete certain data in the interest of efficiency, to be used with telemedicine video communications.

4.3.7 Data Communications—Non-Interactive

4.3.7.1 Text Messages

Table 18: EMS Data Communication—Non-Interactive

The communication occurs:	
with whom	Communicate with local and neighboring agencies using e-mail connections, Web browsers, etc. Monitor incident personnel biometric status; traffic status monitors, traffic control devices, and road conditions; hospital and health center status monitors; patient-history smart cards as carried by patient; and state public health services and the Centers for Disease Control and Prevention (CDC) Health Alert Network (HAN) services.
for what purpose	Text data communications are used to access current and archived computerized information, to establish the identity and medical background of patients, and communicate with responsible medical and incident personnel; to provide EMS personnel with data on special hazards, such as toxic materials, at the site that may affect the diagnosis and treatment of patients; and to provide EMS personnel with the medical history and records from a patient's portable medical records devices. These communications also provide the EMS personnel on scene with the real-time biometric status of firefighters, search and rescue team members, and others on scene who are operating under hazardous conditions and whose vital statistics are to be monitored. They also provide EMS ambulance personnel with real-time traffic status (such as Intelligent Transportation System information for traffic congestion updates), and provide drivers with the capability to control traffic lights during an emergency. Further, these communications provide EMS ambulance personnel with hospital updates on diversion status, capability status, and resource availability, such as ER and cardiac care, and display the medical history of patients from patients' smart cards, which would contain information about allergies, prescription drug use, heart pacemaker, etc.

Table 18: EMS Data Communication—Non-Interactive (Continued)

The communication occurs:	
with what special constraints	Much of this information needs to be secured to protect privacy concerns and the chain-of-command for lifesaving procedures. Communications must include the ability to access state public health information services as well as the CDC HAN, and need to ensure that EMS systems and public health systems are not "stove-piped" solutions.

4.3.7.2 Image Communications

Few "non-interactive" image communications are needed by EMS field personnel, although pictures of buildings to which EMS may be dispatched would be useful for location identification.

4.3.7.3 Video Communications

No "non-interactive" video communications are needed by the EMS field personnel.

4.4 Law Enforcement

4.4.1 Routine Operability and Day-to-Day Interoperability

Day-to-day activities are in the class of general or routine LE services, such as traffic law and motor vehicle enforcement, crime prevention efforts, patrol operations, search and rescue operations, domestic disturbances, arrest warrant executions, investigative operations, court security, administrative communications, and information exchange.

The next sections breakdown LE by local, tribal, state, and Federal agencies.

4.4.1.1 Local Law Enforcement Agencies

These activities take place in office, patrol car, and pedestrian environments, and within building structures. The area of operation is usually within the agency's jurisdictional boundaries and usually within the nominal communications range of the local radio infrastructure. Operations may extend to the remote edges of the jurisdiction and to in-building situations, as well as to irregular operations into neighboring jurisdictions. The routine operations also include those that bring together LE officials from more than one agency and may involve other public safety providers, such as fire response and EMS units. Examples would include: a multi-car accident with injuries and possible deaths on an interstate highway in an urban area requiring state patrol, local police, fire personnel, and EMS response; a burglary in progress and suspect pursuit across several jurisdictions; and a search and rescue of a private plane crash on a remote mountainside.

4.4.1.2 Tribal Law Enforcement Agencies

Tribally operated LE agencies operate in a variety of environments, from large land area law enforcement regions (e.g., the Navajo Nation LE department covers 22,000 square miles in three states) to urban city enforcement (such as the Reno, Nevada, Police Department). Most of these activities are similar to those of local or county LE.

4.4.1.3 Statewide Law Enforcement Agencies

Most of these activities are centered on patrol car monitoring of vehicles on major state highways, although responsibilities are statewide. Some states have state police functions that mimic local law enforcement tasks but occur on a statewide level.

4.4.1.4 Federal Law Enforcement Agencies

Federal activities take place in airports, seaports, border crossings, along borders, in Federal courts and prisons, at Federal buildings and property, and in rural and urban areas. Federal agencies require that most voice communications use Type 1 National Security Agency-approved end-to-end encryption. To support the Federal agencies' missions, communications is needed along all borders, along major highways, and in the metropolitan areas of major cities.

4.4.2 Task Force

Task force operations are those that bring together LE officials from more than one agency and may involve other public safety providers, such as fire and EMS units. Examples include an arson task force formed to review the causes of a suspicious fire; a joint drug/alcohol/firearm enforcement operation by local police, county sheriff, and Federal agents; and a terrorism task force in continuous operation with multiple local, state, and Federal law enforcement agencies. Such operations may include the use of covert communications placed on a decoy officer or on an officer who has infiltrated a criminal group.

For sporting events and other large public gatherings that can be planned in advance, a coordinated LE response is also required. Field units will typically communicate with command posts established at the site of these events. For this latter class of planned events, this section assumes the same operational needs as day-to-day operations, although they will be expanded in scope.

4.4.2.1 Local Law Enforcement Agencies

Task force situations include officers in patrol cars or on foot. These may involve rapidly changing locations outside of nominal local infrastructure communications, including remote locations where no communications infrastructure is available, areas where in-building communications is required, and areas where communications is available only from neighboring infrastructures.

4.4.2.2 Tribal Law Enforcement Agencies

Operations include tribal LE officers in mobile units, in rural areas, on the street in urban areas, and within buildings. Many situations involve rapid changes in the scene of the operation, in which communications through the infrastructure may be limited or non-existent.

4.4.2.3 Statewide Law Enforcement Agencies

Most situations will involve officers in patrol cars or mobile units. These may involve rapidly changing locations, including remote locations where no communications infrastructure is available, areas where in-building communications is limited, and areas where additional communications capabilities are available from neighboring city or county infrastructures.

4.4.2.4 Federal Law Enforcement Agencies

Task force situations include agents in mobile units or on foot. The situations may involve rapidly changing locations as the incident unfolds. Communications may be needed outside of the agency's

nominal communications infrastructure area, including remote and in-building locations, where direct unit-to-unit radio communication is required.

4.4.3 Mutual Aid

Most situations will involve LE officials in office, car, pedestrian, airborne, or search-and-rescue environments. Mutual aid operations can occur in a wide range of situations, including weather-related events (hurricanes, flooding, tornadoes), natural causes (earthquakes), major explosions (terrorist or accidental), transportation incidents (commercial plane crash), major fires, riots, etc. These large-scale disaster events are not planned. Disaster events are those that stress communications capabilities the most and are discussed in the next sections.

Large-scale disasters requiring mutual aid are characterized by a large number of external agencies and personnel brought in to address the emergency. These include agencies from neighboring regions and states, national organizations, and Federal agencies. Communications among all of these additional personnel will be required, with a temporary command structure, and via existing, still-operational infrastructure and extra, temporary infrastructure. Contacts may include LE, traffic control, fire response, EMS, emergency management, Hazmat units, urban search and rescue, military, National Guard, utility and transportation companies, relief agencies, weather information, temporary housing and food, volunteers, etc., depending on the scale and type of the disaster.

Also falling into the category of mutual aid are extremely large planned events, such as political conventions, the Olympics, and international meetings, where a host state's mutual aid pact is activated in advance. In such events, all response teams will be coordinated. Numbers of special units, such as SWAT and bomb disposal teams, will be staged and must be coordinated. It is anticipated that large amounts of resources will be staged nearby to support these events, including resources to deal with potential disruption and civil unrest related to the event that might occur. The public will expect the provision of day-to-day level services throughout the event, even while the host agency continues to provide the same level of services to the remainder of its jurisdiction.

4.4.4 Voice Communications—Interactive

4.4.4.1 Routine Operability and Day-to-Day Interoperability Operations

Table 19: Law Enforcement Voice Communication—Interactive 1

The communication occurs:		
with whom	**Local law enforcement agencies:**	Coordination with other officers on selected user groups from within agency, selected user groups in neighboring areas, and selected user groups in neighboring agencies. Connect to incident commander, dispatcher, and supervising officers, special task force command officers and other activity participants, or any other persons on a person-to-person basis.
	Tribal law enforcement agencies:	Because criminal jurisdiction over offenses occurring within tribal territories depends upon the particular offense, the offender, the victim, and the location of the offense. Thus, the prevailing jurisdiction, and subsequent communications, may be tribal, state, or Federal.
	Statewide law enforcement agencies:	Other officers on selected user groups across the state, and selected user groups in overlapping areas, particularly counties and cities. The dispatcher and supervising officers, special task force command officers and other participants, or any other persons on a person-to-person basis.
	Federal law enforcement agencies:	Other agents on selected user groups within the agency, with agents of other agencies, and with law enforcement personnel from local, state, and international law enforcement agencies.
for what purpose	These voice calls are for the routine purpose of receiving instructions and assignments from the dispatcher, informing the dispatcher of progress, assisting agents and officers on task force operations and incidents, asking other agents and officers for help or information, keeping current on incidents in neighboring city and county areas, and responding to requests for assistance, etc. They are also to coordinate with assignment dispatch and incident dispatch to determine availability, to assign calls, to decide on routes, and determine disposition. CAD is used to assign resources in some locations.	
with what special constraints	LE administrators need to be able to set access and usage priorities for all users, and to control usage so that only authorized individuals are allowed to talk to one another. Some of the communications, especially those of Federal agents, need to be encrypted for privacy and tactical situations. An “emergency” button on the radio provides for high-priority treatment of emergency calls.	

4.4.4.2 Task Force Interoperability

Table 20: Law Enforcement Voice Communication—Interactive 2

The communication occurs:	
with whom	Other agents and officers or dispatchers involved with the task force incidents. These contacts may be from user groups within the agency, selected user groups in neighboring agencies operating inside or outside the range of their infrastructure, the PSTN, dispatchers and supervising officers, incident task force command officers and other participants, or other individuals on a person-to-person basis. Contacts may include Federal agents; state officers; tribal, local city or county LE; traffic control; fire response; EMS; Hazmat units; special operations; utilities; public works; and transportation.
for what purpose	These calls are to communicate immediate intelligence and coordination with respect to an incident in progress. They may involve agent or officer safety, and the safety of the public.
with what special constraints	These communications must be available with high reliability and rapid, indeed apparently instantaneous, response times. They may need to be encrypted.

4.4.4.3 Mutual-Aid Interoperability

Table 21: Law Enforcement Voice Communication—Interactive 3

The communication occurs:	
with whom	Among agents and officers from various agencies at the incident scene, between the agents and officers with their supervisors, and between the supervisors and the IC.
for what purpose	Communications will be needed to coordinate the activities of large numbers of external workers and local workers, and possibly to reestablish civilian order and safety, at a time when the local infrastructure may or may not be operational.

Table 21: Law Enforcement Voice Communication—Interactive 3 (Continued)

The communication occurs:	
with what special constraints	This may require establishing communications with a large number of local, state, and national agencies and personnel who have been rapidly moved into the disaster area, and with many critical missions that must be performed as soon as possible. Local communications infrastructures (including local telephone service and local LE radio infrastructure) may or may not be operational, with the result that direct unit-to-unit communications may play a critical role. In other situations, there may be no initial infrastructure, such as at a wildfire incident. It is desirable to capture a record of communications when the infrastructure is not available, so temporary communications systems may need to be set up to partially replace non-functioning local systems, as well as to provide communications for a large number of additional workers. Some of these communications should be encrypted. The incident administrators need the ability to rapidly establish high-priority user groups, to validate the users attempting to use the system, to create temporary networks on the fly, and to provide authorizations for those with whom users may have communications. The users need to have access to communications that are seamless and transparent in accordance with their public safety roles and responsibilities.

4.4.5 Voice Communications—Non-Interactive

Table 22: Law Enforcement Voice Communication—Non-Interactive

The communication occurs:	
with whom	All law enforcement agencies may use voice paging and alerting between dispatchers and officers or agents, from dispatchers and task force commanders to task force members, and from dispatchers and mutual aid ICs to mutual aid members.
for what purpose	These voice calls inform the officer or agent of a request for assistance or service, of administrative information, or of other, routine matters. They also provide paging and alerting of task force or mutual aid operations.
with what special constraints	LE administrators need to be able to set access and usage priorities for the non-interactive communications to ensure priority calls receive proper treatment. Some of the communications, especially those of Federal agents, need to be encrypted for privacy and tactical situations. These communications must be available with high reliability and rapid (apparently instantaneous) response times.

4.4.6 Data Communications—Interactive

4.4.6.1 Text Messages

Table 23: Law Enforcement Data Communication—Interactive 1

The communication occurs:	
with whom	Other agents and officers in local and neighboring agencies using directed text messages, and access to local, state, and national databases. These include databases and active files on a wide range of public safety activities from local and state agencies, and other state or Federal information sources. Examples of Federal databases include the Federal Bureau of Investigation's National Crime Information Center (NCIC), the Integrated Automated Fingerprint Identification System, the U.S. Immigration and Customs Enforcement Automated Biometric Identification System, and the Joint Automated Booking System. Communications could also include personnel in other components of the criminal justice system, such as officers in corrections facilities, judges, prosecutors, and defense attorneys.
for what purpose	Text data communications are used for a wide range of functions to access current and archived computerized information on vehicle license plates and driver's licenses, printed updates and supplements to current duty assignments or situations, wants and warrants, stolen properties and vehicles, additional background and criminal histories on particular subjects, etc. Data communications (agent/office-in-a-vehicle capabilities) are used to file reports and traffic citations remotely and electronically, making them rapidly and efficiently available to local and neighboring public safety officials and/or state public safety officials. For a mutual aid operation, text data communications may be needed as a general organizational tool to coordinate the activities of large numbers of external workers and local workers; to help re-impose organization on a chaotic situation; and to organize, catalog, and disseminate a large number of known facts about a current emergency (e.g., lists of survivors and missing persons, damaged infrastructure, and needed supplies). Printed and recorded digital information is particularly valuable to help clarify confusion that immediately follows a disaster.
with what special constraints	For a mutual aid operation, it is necessary to establish communications quickly with a large number of local, state, and national agencies and personnel who have been rapidly moved into the disaster area, with many critical missions that must be performed as soon as possible. Local communications infrastructures (including local telephone service and local LE radio infrastructure) may or may not be operational, so temporary communications systems may need to be set up to partially replace non-functioning local systems, as well as to provide communications for many additional workers. Much of this data needs to be encrypted to protect privacy and ongoing criminal investigations. Access to much of this information is restricted to certain individuals and purposes; the individuals, as well as the information, will have to be authenticated and tracked.

4.4.6.2 Image Communications

Table 24: Law Enforcement Data Communication—Interactive 2

The communication occurs:	
with whom	Communications with local, state, and national databases, various public safety agents and officers in the field, dispatchers, and command officers. Databases include archival databases and active files on a wide range of public safety activities from local and neighboring jurisdictions and agencies, as authorized and required.
for what purpose	The images are transferred for a wide range of purposes, including persons, vehicles, or things that are either being searched for, or which have been found and are in need of identification. Fingerprints taken in the field can be sent in for rapid identification. Maps, drawings, and aerial photographs of buildings, roads, and geographic areas serve a wide range of planning, investigative, traffic control, and search functions. Pictures taken at a scene are useful immediately as planning and tactical tools, and for identification of suspects by witnesses: these pictures are useful later as evidence and for investigatory purposes.
with what special constraints	Encryption will be needed to preserve privacy and to prevent the release of critical data. Access to this information will be restricted to certain individuals and purposes, and will be authenticated and tracked. Some time-critical information will need to be delivered in a short time frame. Other information will be requested only by individuals, but again the information will be needed in a short time to be effective.

4.4.6.3 Video Communications

Table 25: Law Enforcement Data Communication—Interactive 3

The communication occurs:	
with whom	Transmission of video-on-demand between various public safety agents and officers in the field, dispatchers, and command officers; or store and forward on demand and transmit in real-time, the video stored in the agent's vehicle or officer's patrol car. Includes air support downlink from helicopter, and other specialized usages, such as underwater. Transmission to dispatch or IC from private, non-public safety sources, such as schools and banks. Officers, dispatch, or incident commander can access video from private, non-public safety sources, such as schools, banks, area surveillance cameras, news cameras, and traffic cameras.

Table 25: Law Enforcement Data Communication—Interactive 3 (Continued)

The communication occurs:	
for what purpose	Video pictures taken at the scene of a stakeout, a traffic stop, or an arrest, or obtained from surveillance cameras, are useful as evidence or for further investigation to document officer conduct and to send assistance in case of trouble. These recordings may be recorded for later viewing or sent directly to a dispatcher or investigator. Further, video from cameras located to monitor traffic flow provide situation information. For a mutual aid operation, there will be a requirement to rapidly assess damage caused by a disaster, sending on-site views to recovery coordination officials at remote command posts. Real-time video will also be used by robotics operators and search-and-rescue teams when the situation is too risky for personnel, and to rapidly assess the current situation.
with what special constraints	Real-time transmission is needed if the video is used to provide agent or officer assistance. If the video is used for the surveillance of a large building or field, for example, the resolution may not be sufficient to determine details of the people or objects in the frames. If the video is used during traffic stops or drug raids, for example, the resolution should be detailed enough to read license plates and to determine an individual's characteristics.

4.4.7 Data Communications—Non-Interactive

4.4.7.1 Text Messages

Table 26: Law Enforcement Data Communication—Non-Interactive 1

The communication occurs:	
with whom	Communications with local and neighboring agencies using e-mail connections, Web browsers, etc.; with dispatchers and supervisors via short messages; with other agents and officers in local and neighboring agencies using e-mail connections; and with databases using Web browsers. Communicate with status monitors or by telemetry from task force site monitors to the commander or other central location. Communicate with IC at major events, including locations and status information.

Table 26: Law Enforcement Data Communication—Non-Interactive 1 (Continued)

The communication occurs:	
for what purpose	Text data communications provide continuous location and status information on vehicles and personnel; e-mail messages are used to exchange files, discussions, strategies, etc.; databases are used to locate information, as well as to provide reports, modify or add entries, etc. Text data might be used to rapidly distribute detailed background information, resource and personnel information, or planning information among a number of incident participants, in situations when the participants are not required to respond to the communications. Status monitors include up-to-date reports on traffic congestion, weather forecasts, fire and water states, etc. Telemetry data might include weather and environmental information, such as toxic gas content. Reports may be used to support LE interaction with other components of the criminal justice system, such as booking a suspect into a jail, or obtaining a search warrant. Status monitors include up-to-date reports on traffic congestion, weather forecasts, fire and water states, etc. Such communications also include input to traffic control systems and Intelligent Transportation Systems, such as variable message displays.
with what special constraints	Much of this data needs to be encrypted to protect privacy concerns and ongoing criminal investigations.

4.4.7.2 Image Communications

Table 27: Law Enforcement Data Communication—Non-Interactive 2

The communication occurs:	
with whom	Dissemination of images from a dispatcher to a large group of agents, patrol officers, and law enforcement personnel, and vice-versa (e.g., the picture of a missing child can be transmitted from an officer to a dispatcher). Video displays on highways could be used for Amber Alerts.
for what purpose	The images of missing children, mug shots of wanted individuals, etc., are transferred to field personnel to ensure many individuals are able to watch for and recognize missing or wanted people. Images are displayed on highways signs and cellular telephones so citizens can see the subject of Amber Alerts or similar alerts.
with what special constraints	Encryption will be needed to preserve privacy and prevent the release of critical data. Access to this information will be restricted to certain individuals and purposes, and will be authenticated and tracked. Some time-critical information, such as an image of an abducted child, will need to be delivered in a short time to all law enforcement personnel.

4.4.7.3 Video Communications

Table 28: Law Enforcement Data Communication—Non-Interactive 3

The communication occurs:	
with whom	Transmission of video from field sites to a central location, to a dispatcher, or to an investigator.
for what purpose	Surveillance video from within an active crime scene could be relayed to officers responding to the incident.
with what special constraints	Real-time review of the video pictures may not be required, and the video may be used for archival or evidentiary purposes. If the video is used for surveillance of a large building or field, for example, the required resolution may be low. If the video is for a stakeout to observe who enters or leaves a building, for example, the required resolution may be high. Video quality must be good enough to generate a still picture.

5 System of Systems

This section describes, in detail, the network topology that will be used in meeting the requirements set forth in Section 6, Section 7, and Section 8. Specifically, this section defines the network interfaces, both wired and wireless, and defines the links between the interfaces.

5.1 Network Description

The communications systems must be integrated with the public safety user's operations. For example, as a police officer leaves a patrol car to respond to a traffic stop or to investigate a domestic dispute, the critical communications capabilities, whether voice or data, must remain with the officer. As a firefighter enters a burning building, the biometric monitoring devices, the equipment status devices, and the firefighter's location device must indicate to the IC the firefighter's status and location at all times. These wireless devices must work in a variety of networks. Together, they will form the system of systems (see Figure 1). They will have the following natural network hierarchy.

a. **PAN**—The PAN for a first responder can take on many different forms. Primarily, it is intended to represent a set of devices on the person of a first responder that communicate with the first responder's PSCD as necessary. The devices on a PAN will include such items as heart rate monitors, location sensors, etc. This information could, and would in many cases, be transmitted to other areas of the network.

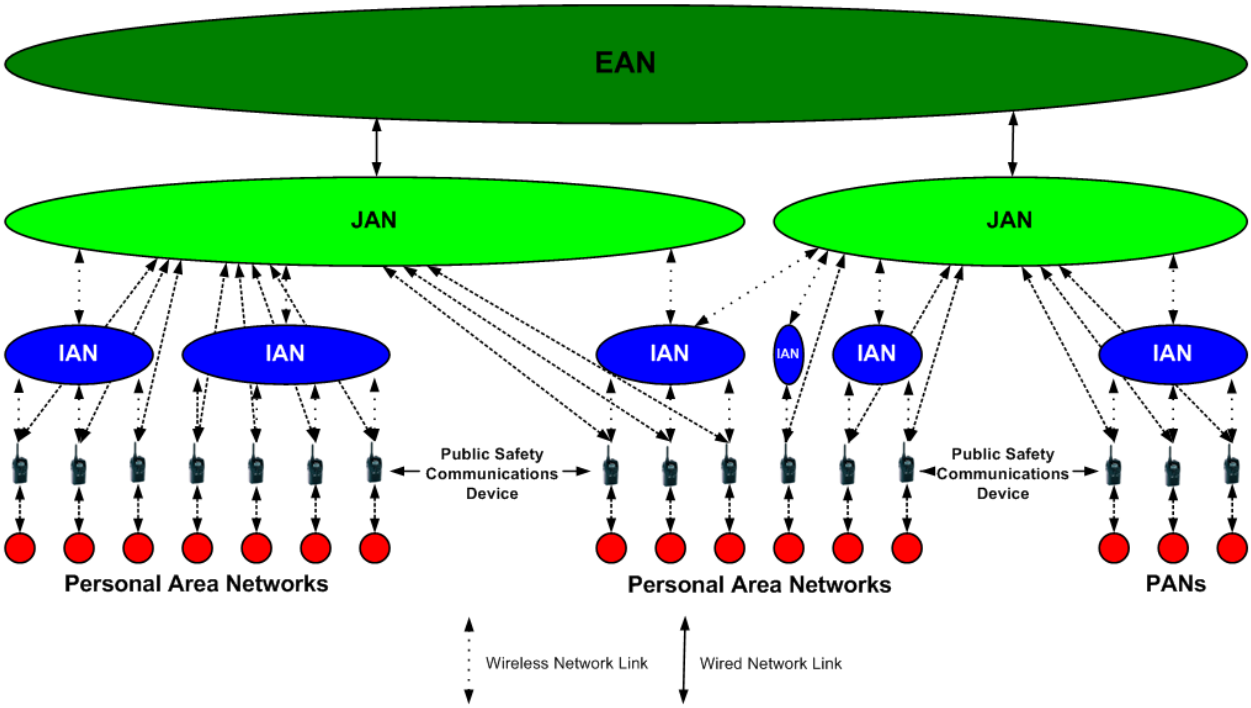
b. **IAN**—An IAN is a network created for a specific incident. This network is temporary in nature; it is typically centered on a wireless access point attached to the first responders' vehicle, or an IAN node. Multiple vehicles therefore dictate multiple nodes, all of which coordinate their coverage and transmissions seamlessly and automatically. This network scales to the size of the incident, from a local traffic stop, to a large-scale, multi-discipline, multi-jurisdiction event. Thus, when an incident is dispersed across a large geographic area, it is expected that the IAN will also leverage the JANs and EANs as needed.

c. **JAN**—The JAN is the main communications network for first responders. It handles any IAN traffic that needs access to the general network, and provides the connectivity to the EAN. This network is more permanent in nature, and is typically made up of JAN nodes, or communications towers. Additionally, it is the component of the network that will handle any and all communications from a first responder's PSCD, should a connection with the local IAN fail or be otherwise unavailable.

d. **EAN**—The local systems are, in turn, linked with county, regional, state, and national systems or EANs. It is expected that this network could be both wired and wireless, depending on the type of infrastructure deployed in the area, e.g., microwave point-to-point, fiber.

Each of the area networks described above are logical concepts. This is an important point to make, as an IAN can be made up of both IAN nodes as well as JAN nodes. Conversely, a JAN can be made up of JAN nodes in addition to an EAN link to connect geographically diverse JAN nodes. This concept is explored further in Section 5.3.

Figure 1: Natural Network Hierarchy



Because public safety operations are usually conducted in the field and emergency operations must take place in the vicinity of the emergency, the networks must allow for mobile members and/or the networks themselves must be mobile and temporary in nature. They must be dynamic and scalable to allow new resources to come onto a temporary network, and they must allow temporary networks to integrate with larger temporary or fixed networks.

Additionally, the management of these networks must allow for automated management as well as user-led management, when necessary and as local policy dictates.

5.2 Network Diagram

The following network diagram shows all of the links and interfaces that have been identified at this point based on the scenarios and requirements discussed in this document.

Figure 2: Link Diagram

In the preceding figure, the dotted lines denote a wireless connection, and the solid lines denote a wired or wireless connection. A red circle around the end of a link denotes a distinct interface, whether wired or wireless.

The following table provides a short description of each link.

Table 29: Network Diagram Link Descriptions

Link	Represents the Connection Between
Link 1	The PAN of the first responder and the first responder's PSCD. The data collected by the sensors on the first responder's body is transmitted aggregately to the PSCD. The main considerations in sizing this link are the amount of data to be transmitted, the distance the transmission must travel, and interference from outside sources, including other first responders' PANs.
Link 2	The first responder's PSCD and the first responder vehicle (FRV) when the PSCD is in range of the vehicle's node, creating part or all of the IAN. Links 2, 3, and 4 all use the same interface, but separating the links allows for separate performance specifications for each.
Link 3	PSCD to PSCD communications. This link is used in peer-to-peer communications. Links 2, 3, and 4 all use the same interface, but separating the links allows for separate performance specifications for each.
Link 4	FRV-to-FRV communications. Links 2, 3, and 4 all use the same interface, but separating the links allows for separate performance specifications for each.
Link 5	The first responder's PSCD and JAN infrastructure. This connection is only used when the first responder is out of range of an IAN node created by an FRV node or some other IAN node. This means a first responder on foot would use this link all the time, while a first responder operating out of a vehicle would only use this link when the connection between the first responder's PSCD and the vehicle IAN node were unavailable.
Link 6	The FRV and the JAN infrastructure. This link is used for the same traffic that link 5 is used for, the primary differentiator being the location of the first responder with respect to an FRV. As was described for link 5, if the first responder is within transmission distance of the vehicle node, data is passed over the vehicle IAN node before being transmitted to the JAN node; otherwise, the first responder's PSCD transmits directly to the JAN node.
Link 7	The JAN infrastructure pieces. While this connection is most likely also connected to the dispatch central office, it provides the capability to describe traffic that does not route itself through the dispatch central office.
Link 8	The dispatch central office and JAN infrastructure.
Link 9	The dispatch central office and a wider network. It is through this link that DMV, NCIC, PSTN, and other extranet queries will be forwarded.
Link 10	This link denotes FRV-to-vehicle communications over the JAN interface without passing through a JAN tower node. In other words, this link accommodates ad hoc networking using the JAN interface.

Each of the interfaces identified in Figure 2 is unique to the network. The following table provides a short description for each interface.

Table 30: Network Diagram Interface Descriptions

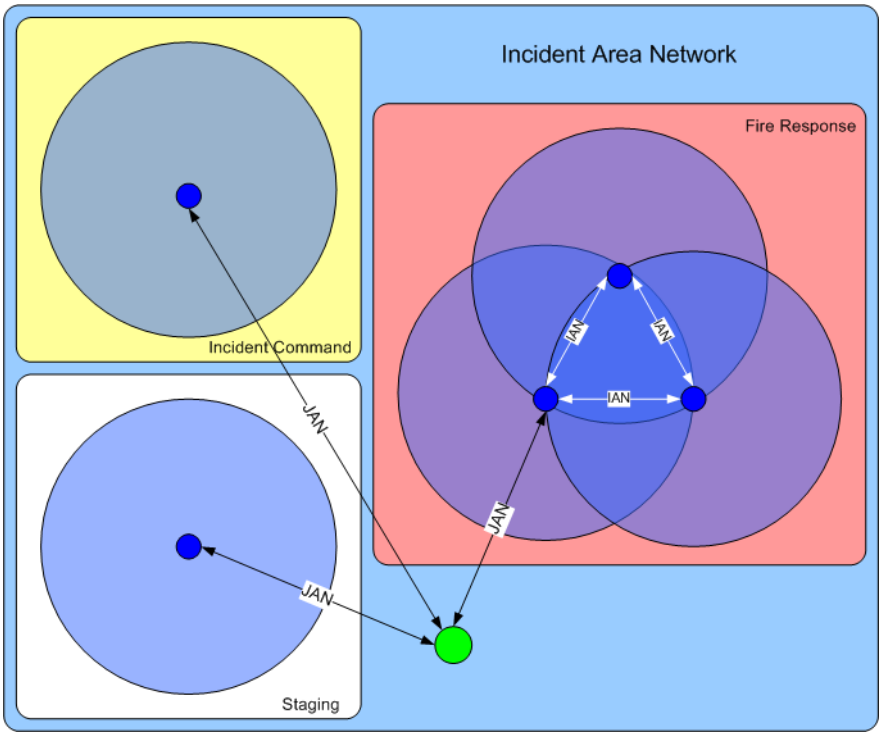
Interface	Is Specified As
Interface 1	The interface that handles the aggregate transmissions to or from a first responder's PAN to or from the PSCD. This is a wireless interface unless the PSCD is integrated directly into the PAN.
Interface 2	The interface that handles transmission to or from the PSCD/FRV to or from the PSCD/FRV via the IAN. This is a wireless interface.
Interface 3	The interface that handles transmissions to or from the PSCD/FRV to or from the fixed/mobile infrastructure via the JAN. This interface also accommodates FRV-to-FRV communications as needs dictate. This is a wireless interface.
Interface 4	The interface on a piece of fixed/mobile infrastructure that handles transmissions to or from another piece of fixed/mobile infrastructure. This interface can be wired or wireless.
Interface 5	The interface that handles transmissions to or from a piece of fixed/mobile infrastructure to or from the local dispatch central office. This interface can be wired or wireless.
Interface 6	The interface to or from other network types, including the PSTN, other jurisdictions, the public Internet, and so forth to or from the dispatch central office. This is a wired interface.

5.3 Network Topology

The four area networks (PAN, IAN, JAN, and EAN) discussed in Section 5.1 are logical constructs that provide context for understanding different aspects of a public safety communications network. Each area network type is created using nodes. For example, an IAN can be created using a grouping of IAN nodes on first responder vehicles. The PAN is a combination of devices on the person of a first responder. The JAN will most likely be constructed from JAN nodes on towers, akin to today's LMR towers. And while these examples are the likely cases, they are not intended to be limiting.

Using the scenario Section 3.5 describes, Figure 3 and Figure 4 show two IAN examples to further describe the flexibility of the network hierarchy that Figure 1 presents.

Figure 3: Incident Area Network with JAN Tower Node



In Figure 3, the smaller dark blue circles indicate IAN nodes. These nodes are notionally placed on top of FRVs. The larger light blue circles indicate coverage for the IAN nodes on the vehicles. The light green circle indicates a JAN tower node. The three boxes indicate geographically diverse areas for the scenario. As shown, the light yellow box denotes the location of Incident Command, the white box showing the staging area as separate from Incident Command, while the light red box shows the first response area. As indicated, the black arrows denote a JAN communications link while the white arrows denote an IAN communications link.

The three boxes indicate geographically diverse areas for the scenario. As shown, the light yellow box denotes the location of incident command, the white box showing the staging area as separate from incident command, while the light red box shows the first response area. As indicated, the black arrows denote a JAN communications link, while the white arrows denote an IAN communications link.

Based on the diagram, the light blue box shows the logical IAN that is created to combat a chemical plant explosion. It is a logical description because there are three groups of IAN nodes that are connected together through a JAN tower node that is acting as a notional repeater in addition to providing backhaul to the rest of the communications network as needed. So, in this example, the IAN includes three separate groups of IAN nodes connected together via a JAN tower node.

Figure 4: Incident Area Network without a JAN Tower

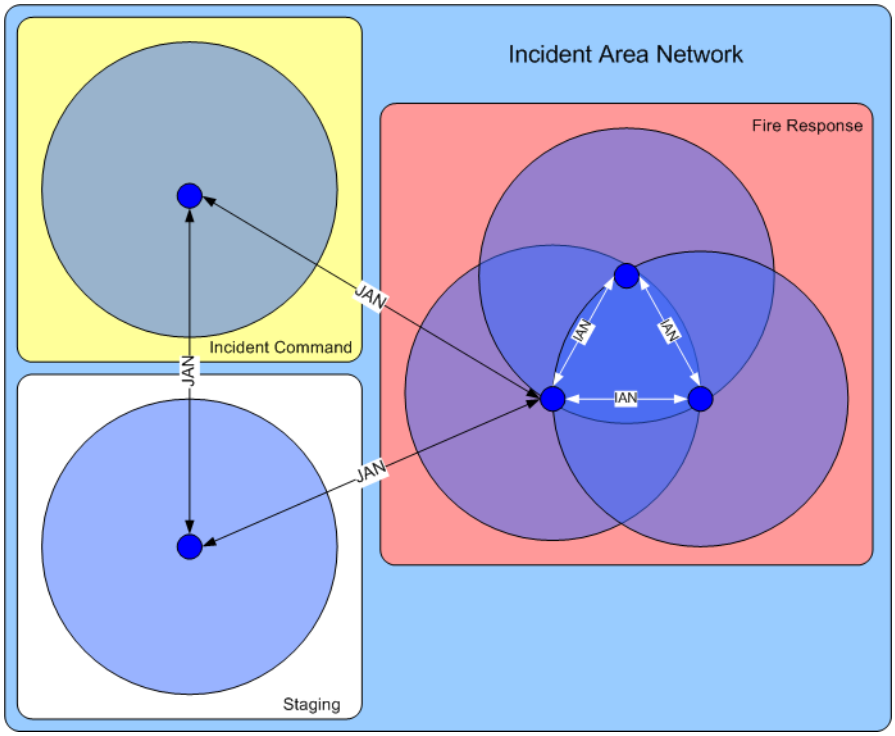


Figure 4 is similar to Figure 3, but lacks a JAN tower node. Figure 4 shows that, in the absence of a JAN tower node to act as a repeater connecting the three IAN node clusters, the JAN interfaces on the vehicles can create an ad hoc network amongst themselves to relay traffic to and from the three areas of the incident.

This page intentionally left blank.

6 Application and Services Functional Requirements

This section of the PS SoR defines the requirements for the application and services, and their feature sets. These feature sets include: applications, security, including physical security, operations, and design methodology.

Key to this section is the concept of "class of service." A class of service is a logical grouping of applications and services that share similar performance requirements. For instance, one class of service may be a grouping of jitter-sensitive, highly interactive traffic, while another class of service may consist of jitter-resistant, non-interactive traffic. Each grouping of applications and services, or class of service, can then have network performance requirements applied to the class as opposed to the individual application or service. Applications define the specific class of service that applies to each application or service. Section 8 describes the associated class of service network performance requirements.

6.1 Applications

The requirements in this section apply to all network levels and all applications and services defined for each level. Each of the applications defined in this section will have an accompanying quality of service section defined in later versions of the document.

Matrix 1: Network Congestion Management Requirements

PS SoR Section 6.1 Requirement #	Qualitative Requirement Description	Additional Information
1	Where possible, applications and services must support rate reduction techniques to reduce the network bandwidth used during congested conditions.	

6.1.1 Personal Area Network

This section defines the classes of service and their associated applications for the PAN. The class of service for these applications will be defined by local policy and thus must be capable of modification.

6.1.1.1 Class of Service 0

This class of service is meant to serve emergency traffic originating from devices on the PAN.

Matrix 2: Personal Area Network Requirements 1

PS SoR Section 6.1.1.1 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support creation and implementation of automated emergency triggers, e.g., if a bulletproof vest detects an impact or a firefighter's helmet is impacted, it can originate a message to appropriate parties.	Using the same example, the officer could have a response to a bullet impact on his or her vest preprogrammed, such that if the vest detects an impact, it sends a message to the appropriate parties without the officer needing to initiate the message. In another example, debris from a fire striking a firefighter's helmet could also trigger an alarm.
2	Where possible, applications and services in this class of service must support rate reduction techniques to reduce the network bandwidth used during congested conditions to ensure delivery.	

6.1.1.2 Class of Service 1

This class of service is meant to serve traffic originating from devices attached to the PAN.

Matrix 3: Personal Area Network Requirements 2

PS SoR Section 6.1.1.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support real-time transmission of vital statistics of objects on the PAN, e.g., the heart rate of an LE officer and the oxygen level of an oxygen tank for a firefighter.	

6.1.2 Incident Area Network

This section defines the classes of service and their associated applications for the IAN.

6.1.2.1 Class of Service 0

This class of service is meant to service real-time, jitter-sensitive, high-interaction applications, such as voice or video teleconferencing. These applications will need a separate queue with preferential servicing and traffic grooming.

Matrix 4: Incident Area Network Requirements 1

PS SoR Section 6.1.2.1 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support full-duplex, peer-to-peer, **mission-critical** voice communications in which two or more participants are involved. The session must allow for late entry. User identification must be a feature of the service.	
2	The network must support full-duplex, peer-to-peer, **mission-critical** video in which two or more participants are involved. The session must allow for late entry. User identification must be a feature of the service.	Video in this context includes surveillance, tactical, infrared, and telemedicine. It also includes video teleconferencing.

6.1.2.2 Class of Service 1

This class of service is meant to service real-time, jitter-sensitive, interactive applications, such as voice or video teleconferencing. These applications will need a separate queue with preferential servicing and traffic grooming.

Matrix 5: Incident Area Network Requirements 2

PS SoR Section 6.1.2.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support full-duplex, peer-to-peer voice communications in which two or more participants are involved. The session must allow for late entry. User identification must be a feature of the service.	
2	The network must support full-duplex, peer-to-peer, video in which two or more participants are involved. The session must allow for late entry. User identification must be a feature of the service.	Video in this context includes surveillance, tactical, infrared, and telemedicine. It also includes video teleconferencing.

6.1.2.3 Class of Service 2

This class of service is meant to service transaction data that is highly interactive, such as signaling for voice or video teleconferencing. These applications will need a separate queue with drop priority.

Matrix 6: Incident Area Network Requirements 3

PS SoR Section 6.1.2.3 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support a signaling protocol that is capable of providing session control for both voice and video applications, as well as instant messaging. Additionally, this signaling protocol must be capable of establishing presence on the network.	This protocol will support both mission-critical and non-mission-critical applications.

6.1.2.4 Class of Service 3

This class of service is meant to service transaction data that is interactive, such as an NCIC query. These applications will need a separate queue with drop priority.

Matrix 7: Incident Area Network Requirements 4

PS SoR Section 6.1.2.4 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support peer-to-peer instant messaging.	
2	The network must support automated database transactions.	This type of requirement implies no human interaction or human impetus in the start of an automated query; e.g., license plate recognition software must be able to automatically query a database using the parsed information from the input data source.
3	The network must support database transactions.	Criminal database queries, such as criminal records, NCIC, arrest reports, incident reports, and other information maintained by local, tribal, state, and Federal agencies. Medical database queries for patient history or responder medical history.

6.1.2.5 Class of Service 4

This class of service is meant to service low-loss traffic only, such as short transactions, bulk data, or video streaming. These applications will need a long queue with drop priority.

Matrix 8: Incident Area Network Requirements 5

PS SoR Section 6.1.2.5 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support voice paging in which the transmission is sent to one or more participants.	
2	The network must support bulk file transfer.	Examples of content in which this would be beneficial include, but are not limited to, satellite imagery, building floor plans, GIS overlays, surveillance camera still shots etc.
3	The network must support near-real-time video streaming.	Examples of equipment for which this would be beneficial include, but are not limited, to infrared cameras carried by firefighters and surveillance cameras.
4	The network must support three-dimensional geolocation information transmissions.	Any object on the network must be capable of transmitting this type of information. A quantitative resolution will need to be defined for this requirement.
5	The network must support the status queries of devices from any authorized source and from any location.	

6.1.2.6 Class of Service 5

This class of service is meant to service traditional applications of default networks. These applications will need a separate queue with the lowest priority.

Matrix 9: Incident Area Network Requirements 6

PS SoR Section 6.1.2.6 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support World Wide Web browser-based applications.	

Matrix 9: Incident Area Network Requirements 6 (Continued)

PS SoR Section 6.1.2.6 Requirement #	Qualitative Requirement Description	Additional Information
2	The network must support e-mail.	

6.1.3 Jurisdiction Area Network

This section defines the classes of service and their associated applications for the JAN.

6.1.3.1 Class of Service 0

This class of service is meant to service real-time, jitter-sensitive, high-interaction applications such as voice or video teleconferencing. These applications will need a separate queue with preferential servicing and traffic grooming.

Matrix 10: Jurisdiction Area Requirements 1

PS SoR Section 6.1.3.1 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support full-duplex, peer-to-peer, **mission-critical** voice communications in which two or more participants are involved. The session must allow for late entry. User identification must be a feature of the service.	
2	The network must support full-duplex, peer-to-peer, **mission-critical** video in which two or more participants are involved. The session must allow for late entry. User identification must be a feature of the service.	Video in this context includes surveillance, tactical, infrared, and telemedicine. It also includes video teleconferencing.

6.1.3.2 Class of Service 1

This class of service is meant to service real-time, jitter-sensitive, interactive applications such as voice or video teleconferencing. These applications will need a separate queue with preferential servicing and traffic grooming.

Matrix 11: Jurisdiction Area Requirements 2

PS SoR Section 6.1.3.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support full-duplex, peer-to-peer, voice communications in which two or more participants are involved. The session must allow for late entry. User identification must be a feature of the service.	
2	The network must support full-duplex, peer-to-peer video in which two or more participants are involved. The session must allow for late entry. User identification must be a feature of the service.	Video in this context includes surveillance, tactical, infrared, and telemedicine. It also includes video teleconferencing.

6.1.3.3 Class of Service 2

This class of service is meant to service transaction data that is highly interactive such as signaling for voice or video teleconferencing. These applications will need a separate queue with drop priority.

Matrix 12: Jurisdiction Area Requirements 3

PS SoR Section 6.1.3.3 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support a signaling protocol that is capable of providing session control for both voice and video applications, as well as instant messaging. Additionally, this signaling protocol must be capable of establishing presence on the network.	This protocol will support both mission-critical and non-mission-critical applications.

6.1.3.4 Class of Service 3

This class of service is meant to service transaction data that is interactive, such as an NCIC query. These applications will need a separate queue with drop priority.

Matrix 13: Jurisdiction Area Requirements 4

PS SoR Section 6.1.3.4 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support peer-to-peer instant messaging.	
2	The network must support automated database transactions.	This type of requirement implies no human interaction or human impetus in the start of an automated query; e.g., license plate recognition software must be able to automatically query a database using the parsed information from the input data source.
3	The network must support database transactions.	Criminal database queries, such as criminal records, NCIC, arrest reports, incident reports, and other information maintained by local, tribal, state, and Federal agencies.

6.1.3.5 Class of Service 4

This class of service is meant to service low-loss traffic only, such as short transactions, bulk data, or video streaming. These applications will need a long queue with drop priority.

Matrix 14: Jurisdiction Area Requirements 5

PS SoR Section 6.1.3.5 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support voice paging in which the transmission is sent to one or more participants.	
2	The network must support bulk file transfer.	Examples of content in which this would be beneficial include, but are not limited to, satellite imagery, building floor plans, GIS overlays, and surveillance camera still shots.

Matrix 14: Jurisdiction Area Requirements 5 (Continued)

PS SoR Section 6.1.3.5 Requirement #	Qualitative Requirement Description	Additional Information
3	The network must support near-real-time video streaming.	Examples of where this would be beneficial include, but are not limited to, infrared cameras carried by firefighters and surveillance cameras.
4	The network must support three-dimensional geolocation information transmissions.	Any object on the network must be capable of transmitting this type of information. A quantitative resolution will need to be defined for this requirement.
5	The network must support the status queries of devices from any authorized source and from any location.	

6.1.3.6 Class of Service 5

This class of service is meant to service traditional applications of default networks. These applications will need a separate queue with the lowest priority.

Matrix 15: Jurisdiction Area Requirements 6

PS SoR Section 6.1.3.6 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support World Wide Web browser-based applications.	
2	The network must support e-mail.	

6.1.4 Extended Area Network

This section defines the classes of service and their associated applications for the EAN.

6.1.4.1 Class of Service 0

This class of service is meant to service real-time, jitter sensitive, high interaction applications such as voice or video teleconferencing. These applications will need a separate queue with preferential servicing and traffic grooming.

Matrix 16: Extended Area Network Requirements 1

PS SoR Section 6.1.4.1 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support full-duplex, peer-to-peer, **mission-critical** voice communications in which two or more participants are involved. The session must allow for late entry. User identification must be a feature of the service.	
2	The network must support full-duplex, peer-to-peer, **mission-critical** video in which two or more participants are involved. The session must allow for late entry. User identification must be a feature of the service.	Video in this context includes surveillance, tactical, infrared, and telemedicine. It also includes video teleconferencing.

6.1.4.2 Class of Service 1

This class of service is meant to service real-time, jitter sensitive, interactive applications such as voice or video teleconferencing. These applications will need a separate queue with preferential servicing and traffic grooming.

Matrix 17: Extended Area Network Requirements 2

PS SoR Section 6.1.4.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support full-duplex, peer-to-peer, voice communications in which two or more participants are involved. The session must allow for late entry. User identification must be a feature of the service.	
2	The network must support full-duplex, peer-to-peer video in which two or more participants are involved. The session must allow for late entry. User identification must be a feature of the service.	Video in this context includes surveillance, tactical, infrared, and telemedicine. It also includes video teleconferencing.

6.1.4.3 Class of Service 2

This class of service is meant to service transaction data that is highly interactive, such as signaling for voice or video teleconferencing. These applications will need a separate queue with drop priority.

Matrix 18: Extended Area Network Requirements 3

PS SoR Section 6.1.4.3 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support a signaling protocol that is capable of providing session control for both voice and video applications, as well as instant messaging. Additionally, this signaling protocol must be capable of establishing presence on the network.	This protocol will support both mission-critical and non-mission-critical applications.

6.1.4.4 Class of Service 3

This class of service is meant to service transaction data that is interactive, such as an NCIC query. These applications will need a separate queue with drop priority.

Matrix 19: Extended Area Network Requirements 4

PS SoR Section 6.1.4.4 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support peer-to-peer instant messaging.	
2	The network must support automated database transactions.	This type of requirement implies no human interaction or human impetus in the start of an automated query; e.g., license plate recognition software must be able to automatically query a database using the parsed information from the input data source.
3	The network must support database transactions.	Criminal database queries, such as criminal records, NCIC, arrest reports, incident reports, and other information maintained by local, tribal state, and Federal agencies.

6.1.4.5 Class of Service 4

This class of service is meant to service low-loss traffic only, such as short transactions, bulk data, or video streaming. These applications will need a long queue with drop priority.

Matrix 20: Extended Area Network Requirements 5

PS SoR Section 6.1.4.5 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support voice paging in which the transmission is sent to one or more participants.	
2	The network must support bulk file transfer.	Examples of content in which this service would be beneficial include, but are not limited, to satellite imagery, building floor plans, GIS overlays, and still shots by surveillance camera.
3	The network must support near-real-time video streaming.	Examples of where this would be beneficial include, but are not limited to, infrared cameras carried by firefighters, and surveillance cameras.
4	The network must support three-dimensional geolocation information transmissions.	Any object on the network must be capable of transmitting this type of information. A quantitative resolution will need to be defined for this requirement.
5	The network must support status queries of devices from any authorized source from any location.	

6.1.4.6 Class of Service 5

This class of service is meant to service traditional applications of default networks. These applications will need a separate queue with the lowest priority.

Matrix 21: Extended Area Network Requirements 6

PS SoR Section 6.1.4.6 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support World Wide Web browser-based applications.	

Matrix 21: Extended Area Network Requirements 6 (Continued)

PS SoR Section 6.1.4.6 Requirement #	Qualitative Requirement Description	Additional Information
2	The network must support e-mail.	

6.2 Security

Securing the communications that traverse the architecture defined in these requirements cannot be an afterthought, but a priority. The following requirements need to be considered up front, evaluating each of the other requirements in this document with them in mind.

6.2.1 Authentication

Authentication is the process in which a user is granted access to the network in which a user is identified by the appropriate network resources.

Matrix 22: Security Requirements 1

PS SoR Section 6.2.1 Requirement #	Qualitative Requirement Description	Additional Information
1	A public safety user must be authenticated before the use of all network (PAN, IAN, JAN, and EAN) resources.	
2	A public safety user must be able to authenticate from any geographic location on the network.	This requirement implies that a user must be able to authenticate at any geographic location that is supported by a network adhering to this body of requirements. This does not imply that any user should be able to access services outside that user's normal geographic location without proper authorization.
3	A public safety user's traffic must be tied directly to the user's identity.	Any traffic sent from a public safety user must be verifiable as having been generated by that user, and that user only.

6.2.2 Authorization

Authorization is the process in which a user is granted access to specific resources available through the network (PAN, IAN, JAN, and EAN).

Matrix 23: Security Requirements 2

PS SoR Section 6.2.2 Requirement #	Qualitative Requirement Description	Additional Information
1	A public safety user must be authorized to use specific resources.	
2	A public safety user must be able to gain authorization from any location on the network.	This requirement implies that a user must be able to gain authorization at any geographic location that is supported by a network adhering to this body of requirements. This does not imply that any user should be able to access services outside that user's normal geographic location without proper authorization.
3	A public safety user's authorization must be tied to a role-based access control method.	Roles will be created that predetermine a user's level of access to services; an IC, e.g., will have a different level of services available than will a LE patrol officer. Roles will include, but not be limited to: IC, system security officer, administrator, and operator.

6.2.3 Privacy

Privacy of data involves assuring that only authorized users can access the data.

Matrix 24: Security Requirements 3

PS SoR Section 6.2.3 Requirement #	Qualitative Requirement Description	Additional Information
1	Access to (seeing the contents of) traffic traversing the network must be limited to authorized recipients.	The most common technique used to effect this requirement today is traffic encryption.

Matrix 24: Security Requirements 3 (Continued)

PS SoR Section 6.2.3 Requirement #	Qualitative Requirement Description	Additional Information
2	The traffic must conform to the current Federal Information Processing Standards (FIPS) publication for data privacy, or its equivalent.	For example, this currently implies use of the Advanced Encryption Standard (AES) for data privacy.

6.2.4 Integrity

Data integrity involves assuring that data cannot be modified without detection.

Matrix 25: Security Requirements 4

PS SoR Section 6.2.4 Requirement #	Qualitative Requirement Description	Additional Information
1	The traffic traversing the network must be immune to attacks against its integrity.	The traffic must not be modifiable without detection.
2	The traffic must conform to the current FIPS publication for data integrity, or its equivalent.	For example, this currently implies use of Secure Hash Algorithm (SHA) for data integrity.

6.2.5 Monitoring

The monitoring section defines requirements that enable an administrator to maintain effective control over the network by requiring detailed network observation.

Matrix 26: Security Requirements 5

PS SoR Section 6.2.5 Requirement #	Qualitative Requirement Description	Additional Information
1	The traffic traversing the network must have non-repudiation, i.e., a method of transmitting information where the sender gets proof of delivery and the recipient is certain of the identity of the sender. This has the effect of creating an audit trail. This audit trail must be protected from unauthorized access, modification, and destruction.	The level of non-repudiation must be at least sufficient for transmissions to be entered into court proceedings as evidence. This effective audit trail must provide sufficient detail to reconstruct events occurring on the network. This includes, but is not limited to, all applications and services discussed in Section 6.1

Matrix 26: Security Requirements 5 (Continued)

PS SoR Section 6.2.5 Requirement #	Qualitative Requirement Description	Additional Information
2	The network must be able to be monitored by authorized users in every aspect of its functionality anywhere on the network.	This implies the ability to obtain real-time status of the network from a very granular or detailed level up to and including a macro, jurisdiction-wide level. The information obtained from these status updates will at least provide data regarding the correct operation of the network.
3	The network will log the following events: device failure (including details such as model, serial number, and hardware and software versions); outage start time; diagnosis time; solution implementation time; and time that full functionality was restored.	
4	The network must have a maximum defined period in which, through monitoring and self tests, network component failures are detected and reported	

6.2.6 Attack Prevention and Detection

This section defines a set of requirements for the prevention of attacks against the network, as well as the capability of detecting an attack against the network.

Matrix 27: Security Requirements 6

PS SoR Section 6.2.6 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must be capable of continued operations in the face of a denial of service attack, using any means available.	Denial of service can take the form of a high-power RF jammer, an attack on the Medium Access Control protocol, etc.

Matrix 27: Security Requirements 6 (Continued)

PS SoR Section 6.2.6 Requirement #	Qualitative Requirement Description	Additional Information
2	The network must be immune to traffic flow analysis.	Attackers must be incapable of performing traffic flow analysis. Examples of traffic flow analysis include the incident in which several thousand pizzas were ordered at the Pentagon prior to the start of the first Iraq war, or individuals listening to an encrypted channel who could detect an impending LE action through the increased traffic levels even without understanding the traffic itself.
3	The network must be capable of geolocating the source of an attack against any node on the network.	
4	The network must be capable of effective passive/active attack monitoring and defense deployment	

6.3 Physical Security

This section defines the physical security of the components that make up the system.

Matrix 28: Physical Security Requirements

PS SoR Section 6.3 Requirement #	Qualitative Requirement Description	Additional Information
1	Access to fixed infrastructure must be controlled such that only authorized individuals have access to equipment.	See documents such as the Criminal Justice Information System (CJIS) security policy for additional details on this topic.
2	Access to portable and mobile PSCDs must be controlled such that only authorized individuals have access to equipment.	

6.4 Operations

This section defines the requirements as they pertain to the administrative and maintenance portions of the communications network.

6.4.1 Administrative

This section defines the administrative requirements for the network. The administrative role in this context is similar to that of a system administrator for a networked computing system.

Matrix 29: Operations Requirements 1

PS SoR Section 6.4.1 Requirement #	Qualitative Requirement Description	Additional Information
1	Authorized administrators must be able to create, control, and configure user groups. The users associated with a group can originate from any source where the administrator has nominal access to the user roster.	For the three major types of operations: day-to-day, task force, and mutual aid, the users involved in a group can come from any source appropriate to the mission. This includes users outside the public safety, but properly interfacing through interfaces described in Section 5.2.
2	Authorized administrators must be able to configure and control the following aspects of a user group: on-the-fly user addition and deletion from a group; priorities; roaming; authorizations; security used; transmission power; etc.	This list of configurable elements is not meant to be exhaustive.
3	Authorized administrators must be able to disable a user's access to the network over the air.	
4	Authorized administrators must be able to perform all administrative functions from anywhere on the network.	Whether in the field or at a desk, as long as administrators have authorized access to the network, they can perform their job function.
5	Authorized administrators must be able to disable automated status reporting of objects on the network to prevent unwanted transmissions and to maintain emission control.	
6	Administrator capabilities will include broad policy definitions that will encompass most of the feature and functionality of the network.	

6.4.2 Maintenance

This section defines maintenance requirements for the network. Maintenance involves upgrading, monitoring performance, modification, diagnostics, and other routine aspects of operating a communications network.

Matrix 30: Operations Requirements 2

PS SoR Section 6.4.2 Requirement #	Qualitative Requirement Description	Additional Information
1	Authorized administrators must be able to perform routine maintenance without any user-noticeable degradation of the network.	Such maintenance will consist of replacing failed network objects, performance testing, etc. This is not an exhaustive list.
2	Network self tests and diagnostics must not cause any failure or degradation of any network function.	

6.5 Design Methodology

This section describes design best practices, including the use of commercial off-the-shelf (COTS) technology and standards-based systems. These best practices are overarching requirements for the entire document.

Matrix 31: Design Methodology Requirements

PS SoR Section 6.5 Requirement #	Qualitative Requirement Description	Additional Information
1	COTS technology will be leveraged wherever possible.	Products, standards, etc.
2	The network must be based on standards and must not infringe upon any Intellectual Property Rights (IPR) that are not in the public domain or licensed at a fair and reasonable cost as determined by first responders.	
3	Standards used will be those that provide or take advantage of the broadest possible market base while meeting all of the stated requirements.	

Matrix 31: Design Methodology Requirements (Continued)

PS SoR Section 6.5 Requirement #	Qualitative Requirement Description	Additional Information
4	A well-defined migration path must be created for legacy systems to migrate toward a network satisfying the requirements in this document.	Application of the Public Safety Architecture Framework (PSAF) will accomplish this goal.
5	The network design must provide as much backward compatibility as possible with legacy systems without sacrificing requirements.	

7 Public Safety Communications Device Functional Requirements

This section of the PS SoR defines the requirements for the devices on the public safety communications network that transmit and/or receive information on that network. For the most part, unless stated otherwise, these requirements are optional for the device under which the requirement is detailed.

7.1 First Responder Mobile Communications Device

A first responder mobile communications device is the device that a first responder uses in vehicles. These requirements cover such topics as ergonomics, environmental concerns, and other device-specific requirements.

Matrix 32: First Responder Mobile Communications Device Requirements

PS SoR Section 7.1 Requirement #	Qualitative Requirement Description	Additional Information
1	The device must support biometric identification techniques as a method of identifying a user to the device.	This requirement is provided in the context of the ability to identify a user through an appropriate device. Users in this context can be either first responders or not, the latter in the case of a suspect in a crime. For instance, the first responder could capture pertinent biometric identification information (i.e., a fingerprint) to help identify a suspect. Not all devices must be capable of this feature.
2	The device must support real-time voice commands.	This requirement is designed to provide a high measure of hands-free operation for first responders. Not all devices must be capable of this feature.
3	The device must support voice language translation techniques.	If a member of the public is speaking a foreign language, the first responder's communications device must support a best-effort translation of the language. Additionally, this requirement implies that the first responder then be able to use the device to communicate back to the member of the public. Not all devices must be capable of this feature.

Matrix 32: First Responder Mobile Communications Device Requirements (Continued)

PS SoR Section 7.1 Requirement #	Qualitative Requirement Description	Additional Information
4	The device must support TTY/TDD interfaces (telecommunications for the deaf).	Not all devices must be capable of this feature.
5	The device must support human performance support systems (e.g., online help functions, operator and maintenance training).	All devices must be capable of this feature.
6	The device must be capable of capturing data pertinent to first-responder operations and of sharing this data as necessary, as defined by the administrator.	For example, if an officer arrests a suspect for DUI, when the transporting unit arrives at the jail, the booking officer automatically has access to the data that the arresting officer entered into the device. Or, an EMS first responder could check for helicopter availability for a critical patient. All devices must be capable of this feature.
7	The device must be capable of storing an appropriate amount of data locally on the device.	All devices must be capable of this feature.
8	The device must be capable of generating a transmission to other devices on the network based on those devices' geolocation relative to the transmitting device.	All devices must be capable of this feature.
9	The device must be capable of communications regardless of location: city street, highway, parking garage, high-rise building, airport, airborne, waterborne, etc.	The device must be capable of operating in a diverse set of hostile RF environments while maintaining a minimum level of connectivity, through whatever means are available, such as increased transmission power. Not all devices must be capable of this feature.
10	The device must support a status query from an authorized source.	All devices must be capable of this feature.
11	The device must be capable of supporting low probability of detection techniques.	For example, this feature could be used for covert operations. Not all devices must be capable of this feature.

Matrix 32: First Responder Mobile Communications Device Requirements (Continued)

PS SoR Section 7.1 Requirement #	Qualitative Requirement Description	Additional Information
12	The device must be reprogrammable over the air in a reasonable amount of time. Multiple-device reprogramming can occur simultaneously.	All devices must be capable of this feature.
13	The device must support personality cloning from device to device.	A user, within a limit set by an administrator, will be capable of customizing that user's device. This customization must be reproducible from device to device without the need to reprogram each personality feature individually. This is known as device cloning. All devices must be capable of this feature.
14	The device must support hands-free operation.	All devices must be capable of this feature.
15	The device must support plug-and-play component add-on capabilities.	All devices must be capable of this feature.

7.2 First Responder Portable Communications Device

A first responder portable communications device is the device that a first responder carries when not in the FRV. These requirements include such topics as ergonomics, environmental concerns, and other device specific requirements.

Matrix 33: First Responder Portable Communications Device Requirements

PS SoR Section 7.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The device must support biometric identification techniques as a method of identifying a user to the device.	This requirement is provided in the context of the ability to identify a user through an appropriate device. Users in this context can be both first responders and non-first responders in the case of a suspect in a crime. Not all devices must be capable of this feature, but the network must support the traffic inherent in such a feature.

Matrix 33: First Responder Portable Communications Device Requirements (Continued)

PS SoR Section 7.2 Requirement #	Qualitative Requirement Description	Additional Information
2	The device must support real-time voice commands.	This requirement is designed to provide a high measure of hands-free operation for first responders. Not all devices must be capable of this feature.
3	The device must support voice language translation techniques.	If a member of the public is speaking a foreign language, the first responder's communications device must support a best-effort translation of the language. Additionally, this requirement implies that the first responder then be able to use the device to communicate back to the member of the public. Not all devices must be capable of this feature.
4	The device must support TTY/TDD interfaces.	Not all devices must be capable of this feature.
5	The device must support human performance support systems (e.g., online help functions, operator and maintenance training).	All devices must be capable of this feature.
6	The device must be capable of capturing data pertinent to first responder operations and of sharing this data as necessary, as defined by the administrator.	For example, if an officer arrests a suspect for DUI, when the transporting unit arrives at the jail, the booking officer automatically has access to the data that the arresting officer entered into the device. All devices must be capable of this feature.
7	The device must be capable of storing an appropriate amount of data locally on the device without sacrificing size, weight, and power consumption beyond reasonable expectations.	All devices must be capable of this feature.
8	The device must be capable of generating a transmission to other devices on the network based on those devices' geolocation relative to the transmitting device.	All devices must be capable of this feature.

Matrix 33: First Responder Portable Communications Device Requirements (Continued)

PS SoR Section 7.2 Requirement #	Qualitative Requirement Description	Additional Information
9	The device must be capable of communications regardless of location: city street, highway, parking garage, high-rise building, airport, airborne, waterborne, etc.	The device must be capable of operating in a diverse set of hostile RF environments while maintaining a minimum level of connectivity, through whatever means are available, such as increased transmission power. Not all devices must be capable of this feature.
10	The device must support a status query from an authorized source.	All devices must be capable of this feature.
11	The device must be capable of supporting low probability of detection techniques.	For example, this feature could be used for covert operations. Not all devices must be capable of this feature.
12	The device must be reprogrammable over the air in a reasonable amount of time. Multiple-device reprogramming can occur simultaneously.	All devices must be capable of this feature.
13	The device must support personality cloning from device to device.	A user, within a limit set by an administrator, will be capable of customizing that user's device. This customization must be reproducible from device to device without the need to reprogram each personality feature individually. This is known as device cloning. All devices must be capable of this feature.
14	The device must support hands-free operations.	All devices must be capable of this feature.
15	The device must have a maximum acceptable weight defined separately for each first responder discipline.	All devices must be capable of this feature.
16	The device's shape must be appropriate to the application in which it is used.	All devices must be capable of this feature.
17	The device must have a minimum acceptable battery life defined separately for each first responder discipline.	All devices must be capable of this feature.

Matrix 33: First Responder Portable Communications Device Requirements (Continued)

PS SoR Section 7.2 Requirement #	Qualitative Requirement Description	Additional Information
18	The device must adhere to discipline-specific usability standards. These standards could cover such aspects of the device as button size and screen size.	All devices must be capable of this feature.
19	The device must not introduce undue operator fatigue during continuous usage over a 12-hour period every 24 hours.	An applicable standard could be MIL-STD-1472E or its current equivalent. All devices must be capable of this feature.
20	The device must accommodate use by the 5th percentile female to a 95th percentile male.	An applicable standard could be ASTM F 1166-95a or its current equivalent. All devices must be capable of this feature.
21	The device must conform to a safety standard.	All devices must be capable of this feature. For information, see the FCC OET Bulletin No. 65.[a]
22	The device must support plug-and-play component add-on capabilities.	All devices must be capable of this feature.
23	The device must support citizen use in the event of an emergency.	If a first responder is incapacitated, or otherwise unable to use the PSCD, a passing citizen must be capable of using the PSCD to radio for help.

a.FCC OET Bulletin No. 65 (August 1997): E*valuating Compliance With FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields*, http://www.fcc.gov/oet/rfsafety/ (Cited August 2006).

7.3 Public Safety Sensors

These sensors can range in function from passive chemical sensors on the person of a first responder, to active surveillance cameras, to medical diagnostic devices and biometric sensors. These sensors are, in effect, a part of the public safety intelligence gathering mission, and function to gather information without

direct user intervention when necessary and possible. Their requirements include such topics as ergonomics, environmental concerns, and other device specific requirements.

Matrix 34: Public Safety Sensors Requirements

PS SoR Section 7.3 Requirement #	Qualitative Requirement Description	Additional Information
1	The device must support status queries and other types of communications over the network in real time.	An object can be a first responder's communications device, a passive sensor, RFID tags, smart cards, etc.
2	The device must be capable of generating a transmission to other devices on the network based on those devices' geolocation relative to the transmitting device.	All devices must be capable of this feature.
3	The device must be capable of communications regardless of location: city street, highway, parking garage, high-rise building, airport, airborne, waterborne, etc.	The device must be capable of operating in a diverse set of hostile RF environments while maintaining a minimum level of connectivity, through whatever means are available, such as increased transmission power. Not all devices must be capable of this feature.
4	The device must support a status query from an authorized source.	All devices must be capable of this feature.
5	The device must be capable of supporting low probability of detection techniques.	For example, this feature could be used for covert operations. Not all devices must be capable of this feature.

This page intentionally left blank.

8 Network Functional Requirements

This section describes end-to-end functional requirements specific to each of the four network hierarchies described in Section 5.1 on page 49—the PAN, IAN, JAN, and EAN. End-to-end requirements are applied in a systems, or holistic, fashion to each of the four network hierarchies, rather than breaking down the system into individual subparts with more refined requirements. Each network hierarchy is broken down into varying performance subsections. Lastly, this section identifies interfaces for other types of networks that will connect to the system of systems network hierarchy.

8.1 Network

This section defines requirements specific to each level of the network, including a set of end-to-end requirements. Additionally, it defines priority requirements that cross all network levels.

8.1.1 Priority

This section defines priority requirements that apply to each application and/or service defined in each of the network levels.

Matrix 35: Priority Requirements

PS SoR Section 8.1.1 Requirement #	Qualitative Requirement Description	Additional Information
1	In addition to associating classes of service to an application or service, each packet will be capable of having a priority level associated with it. This prioritization will provide all precedence information for traffic traversing a node.	

8.1.2 Personal Area Network

This section defines the network performance requirements for the PAN.

8.1.2.1 Performance Metrics

This section defines performance metrics for the PAN.

8.1.2.1.1 Class of Service 0

This section defines performance requirements for the PAN that are specific to Class of Service 0.

Matrix 36: Personal Area Network Requirements 1

PS SoR Section 8.1.2.1.1 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 0.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the PAN, IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 0.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 0.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the PAN, IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 0.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the PAN, IAN, JAN, and EAN.

8.1.2.1.2 Class of Service 1

This section defines performance requirements for the PAN that are specific to Class of Service 1.

Matrix 37: Personal Area Network Requirements 2

PS SoR Section 8.1.2.1.2 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 1.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the PAN, IAN, JAN, and EAN.

Matrix 37: Personal Area Network Requirements 2 (Continued)

PS SoR Section 8.1.2.1.2 Requirement #	Qualitative Requirement Description	Additional Information
2	A maximum packet delay variation will be established for this network for Class of Service 1.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 1.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the PAN, IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 1.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the PAN, IAN, JAN, and EAN.

8.1.2.2 Reliability

This section defines reliability requirements for the PAN.

Matrix 38: Personal Area Network Requirements 3

PS SoR Section 8.1.2.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must be capable of handling all of the Class of Service 0 traffic, and any signaling associated with it, even under constrained network conditions.	Pre-emption, over-engineering the network, and other methods are all possible solutions to satisfy this requirement.
2	The network must have a minimum defined reliability. Reliability is defined as the percentage of packets delivered that satisfy Class of Service requirements on the first attempt.	

8.1.2.3 Availability

This section defines the temporal and spatial availability requirements for the PAN.

8.1.2.3.1 Temporal

This section defines the temporal, or time-based, requirements for the PAN.

Matrix 39: Personal Area Network Requirements 4

PS SoR Section 8.1.2.3.1 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must have a defined minimum acceptable temporal availability. Additionally, a clear and cohesive measurement methodology will be defined to address this requirement.	
2	The network must be capable of operating 24 hours a day, 7 days a week, 365 days a year.	

8.1.2.3.2 Spatial

This section defines the spatial, or space-based requirements for the PAN.

Matrix 40: Personal Area Network Requirements 5

PS SoR Section 8.1.2.3.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must have a defined minimum acceptable spatial availability. Additionally, a clear and cohesive measurement methodology will be defined to address this requirement.	This requirement will define how many devices must be capable of operating on a single PAN.

8.1.2.4 Scalability

This section defines horizontal and vertical scalability requirements for the PAN.

8.1.2.4.1 Horizontal

This section defines the horizontal scalability or coverage area for the PAN.

Matrix 41: Personal Area Network Requirements 6

PS SoR Section 8.1.2.4.1 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must be able to scale in terms of coverage area in a very cost-efficient manner, while still meeting all of the requirements for the particular type of network being extended.	The first responder community will determine the affordability of adding more coverage area through a new base station or repeater; such action will not decrease the performance of the network.
2	The network must support the ability to add new infrastructural components into the existing infrastructure and become operational with little to no configuration or setup required.	This requirement defines the concept of the network practicing self discovery of infrastructure devices being added to the network.

8.1.2.4.2 Vertical

This section defines the vertical scalability or number of users for the PAN.

Matrix 42: Personal Area Network Requirements 7

PS SoR Section 8.1.2.4.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must be capable of dynamically scaling to accommodate a growing number of users while not sacrificing any mission-critical services or applications.	This requirement must be adhered to, even in a constrained or congested networking environment.

8.1.2.5 Survivability

This section defines survivability requirements for the PAN. Survivability is the ability of the network to continue operating under adverse or destructive conditions.

Matrix 43: Personal Area Network Requirements 8

PS SoR Section 8.1.2.5 Requirement #	Qualitative Requirement Description	Additional Information
1	The network will not have any single points of failure (SPOF) where economically feasible.	This is an agency-specific requirement calling attention to SPOFs as an engineering reality that must be appropriately weighed and addressed.
2	The network must be capable of self-healing functionality.	This can be likened to a routing protocol that entails routing around a failed link.
3	The network must support ad hoc network creation in the absence of infrastructure.	
4	The network must be able to operate through power fluctuations or power loss for a defined period of time.	

8.1.2.6 Restorability

This section defines the restorability requirements of the PAN. Restorability is the ease of restoring PAN functionality in the event of a catastrophic failure.

Matrix 44: Personal Area Network Requirements 9

PS SoR Section 8.1.2.6 Requirement #	Qualitative Requirement Description	Additional Information
1	The network will have a defined maximum amount of time for restoration or replacement of critical infrastructure.	

8.1.2.7 Spectrum and/or Network Efficiency

This section defines the requirements for spectrum and/or network efficiency for the PAN.

Matrix 45: Personal Area Network Requirements 10

PS SoR Section 8.1.2.7 Requirement #	Qualitative Requirement Description	Additional Information
1	The RF system must be spectrally efficient to a minimum quantifiable degree.	
2	The goodput (information-to-overhead ratio) of the network must be specific to a minimum quantifiable degree.	

8.1.3 Incident Area Network

This section defines the network performance requirements for the IAN.

8.1.3.1 Performance Metrics

This section defines performance metrics for the IAN.

8.1.3.1.1 Class of Service 0

This section defines performance requirements for the IAN that are specific to Class of Service 0.

Matrix 46: Incident Area Network Requirements 1

PS SoR Section 8.1.3.1.1 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 0.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 0.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.

Matrix 46: Incident Area Network Requirements 1 (Continued)

PS SoR Section 8.1.3.1.1 Requirement #	Qualitative Requirement Description	Additional Information
3	A maximum packet loss ratio will be established for this network for Class of Service 0.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 0.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the IAN, JAN, and EAN.

8.1.3.1.2 Class of Service 1

This section defines performance requirements for the IAN that are specific to Class of Service 1.

Matrix 47: Incident Area Network Requirements 2

PS SoR Section 8.1.3.1.2 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 1.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 1.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 1.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the IAN, JAN, and EAN.

Matrix 47: Incident Area Network Requirements 2 (Continued)

PS SoR Section 8.1.3.1.2 Requirement #	Qualitative Requirement Description	Additional Information
4	A maximum packet error ratio will be established for this network for Class of Service 1.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the IAN, JAN, and EAN.

8.1.3.1.3 Class of Service 2

This section defines performance requirements for the IAN that are specific to Class of Service 2.

Matrix 48: Incident Area Network Requirements 3

PS SoR Section 8.1.3.1.3 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 2.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 2.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 2.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the IAN, JAN, and PAN.
4	A maximum packet error ratio will be established for this network for Class of Service 2.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the IAN, JAN, and PAN.

8.1.3.1.4 Class of Service 3

This section defines performance requirements for the IAN that are specific to Class of Service 3.

Matrix 49: Incident Area Network Requirements 4

PS SoR Section 8.1.3.1.4 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 3.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 3.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 3.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 3.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the IAN, JAN, and EAN.

8.1.3.1.5 Class of Service 4

This section defines performance requirements for the IAN that are specific to Class of Service 4.

Matrix 50: Incident Area Network Requirements 5

PS SoR Section 8.1.3.1.5 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 4.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.

Matrix 50: Incident Area Network Requirements 5 (Continued)

PS SoR Section 8.1.3.1.5 Requirement #	Qualitative Requirement Description	Additional Information
2	A maximum packet delay variation will be established for this network for Class of Service 4.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 4.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 4.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the IAN, JAN, and EAN.

8.1.3.1.6 Class of Service 5

This section defines performance requirements for the IAN that are specific to Class of Service 5.

Matrix 51: Incident Area Network Requirements 6

PS SoR Section 8.1.3.1.6 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 5.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 5.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.

Matrix 51: Incident Area Network Requirements 6 (Continued)

PS SoR Section 8.1.3.1.6 Requirement #	Qualitative Requirement Description	Additional Information
3	A maximum packet loss ratio will be established for this network for Class of Service 5.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 5.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the IAN, JAN, and EAN.

8.1.3.2 Reliability

This section defines reliability requirements for the IAN.

Matrix 52: Incident Area Network Requirements 7

PS SoR Section 8.1.3.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must be capable of handling all of the Class of Service 0 traffic, and any signaling associated with it, even under constrained network conditions.	Pre-emption, over-engineering the network, and other methods are all possible solutions to satisfy this requirement.
2	The network must have a minimum defined reliability. Reliability is defined as the percentage of packets delivered that satisfy Class of Service requirements on the first attempt.	

8.1.3.3 Availability

This section defines the temporal and spatial availability requirements for the IAN.

8.1.3.3.1 Temporal

This section defines the temporal, or time-based, requirements for the IAN.

Matrix 53: Incident Area Network Requirements 8

PS SoR Section 8.1.3.3.1 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must have a defined minimum acceptable temporal availability. Additionally, a clear and cohesive measurement methodology will be defined to address this requirement.	
2	The network must be capable of operating 24 hours a day, 7 days a week, 365 days a year.	

8.1.3.3.2 Spatial

This section defines the spatial, or space-based, requirements for the IAN.

Matrix 54: Incident Area Network Requirements 9

PS SoR Section 8.1.3.3.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must have a defined minimum acceptable spatial availability. Additionally, a clear and cohesive measurement methodology will be defined to address this requirement.	This requirement will define how many devices must be capable of operating on a single IAN.

8.1.3.4 Scalability

This section defines horizontal and vertical scalability requirements for the IAN.

8.1.3.4.1 Horizontal

This section defines horizontal, or coverage area, scalability for the IAN.

Matrix 55: Incident Area Network Requirements 10

PS SoR Section 8.1.3.4.1 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must be able to scale in terms of coverage area in a very cost-efficient manner, while still meeting all of the requirements for the particular type of network that is being extended.	The first responder community will determine the affordability of adding more coverage area through a new base station or repeater; this action will not decrease the performance of the network, regardless of the density of such infrastructure pieces.
2	The network must support the ability to add new infrastructural components into the existing infrastructure and become operational with little to no configuration or setup required.	This requirement defines the concept of the network practicing self discovery of infrastructure devices being added to the network.

8.1.3.4.2 Vertical

This section defines vertical, or number of users, scalability for the PAN.

Matrix 56: Incident Area Network Requirements 11

PS SoR Section 8.1.3.4.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must be capable of dynamically scaling to accommodate a growing number of users while not sacrificing any mission-critical services or applications.	This requirement must be adhered to, even in a constrained or congested networking environment.

8.1.3.5 Survivability

This section defines survivability requirements for the PAN. Survivability is the ability of the network to continue operating under adverse or destructive conditions.

Matrix 57: Incident Area Network Requirements 12

PS SoR Section 8.1.3.5 Requirement #	Qualitative Requirement Description	Additional Information
1	The network will not have any SPOF where economically feasible.	This is an agency-specific requirement calling attention to SPOFs as an engineering reality that must be appropriately weighed and addressed.
2	The network must be capable of self-healing functionality.	This can be likened to a routing protocol that entails routing around a failed link
3	The network must support ad hoc network creation in the absence of infrastructure.	
4	The network must be able to operate through power fluctuations or power loss for a defined period of time.	

8.1.3.6 Restorability

This section defines the restorability requirements of the PAN. Restorability is the ease of restoring PAN functionality in the event of a catastrophic failure.

Matrix 58: Incident Area Network Requirements 13

PS SoR Section 8.1.3.6 Requirement #	Qualitative Requirement Description	Additional Information
1	The network will have a defined maximum amount of time for restoration or replacement of critical infrastructure.	

8.1.3.7 Spectrum and/or Network Efficiency

This section defines the requirements for spectrum and/or network efficiency for the IAN.

Matrix 59: Incident Area Network Requirements 14

PS SoR Section 8.1.3.7 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support multicast communications. Multicast occurs when one device sends data across the network to multiple devices. However, depending on the multicast protocol, only nodes that are on the path from the originating device to the receiving device receive and forward the data.	Multicast in this context is used in the same way it is in the Internet Protocol (IP) networking world: multiple parties that are subscribed to a group all receive the same information, much akin to a voice call party line or conference call.
2	The network must support efficient, unique, plug-and-play addressing of every object on the network that receives and/or transmits information of any kind.	
3	The RF system must be spectrally efficient to a minimum quantifiable degree.	
4	The goodput (information-to-overhead ratio) of the network must be specific to a minimum quantifiable degree.	

8.1.3.8 Mobility

This section defines the mobility and/or roaming requirements for the IAN.

Matrix 60: Incident Area Network Requirements 15

PS SoR Section 8.1.3.8 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support first responders from outside jurisdictions using the IAN of a local jurisdiction	It is expected that, at times, first responders from other jurisdictions or disciplines will respond to an incident. It is important that they be capable, based on local policy, of communication on the IAN in place at the incident.

Matrix 60: Incident Area Network Requirements 15 (Continued)

PS SoR Section 8.1.3.8 Requirement #	Qualitative Requirement Description	Additional Information
2	The network must support user transition across multiple IANs while maintaining constant communications and full user functionality.	This requirement includes the ability to roam from IAN to IAN and maintain communications in any jurisdiction or discipline, as defined by local policy.
3	The network must support seamless transition between the IAN and the JAN as a user becomes too far removed from the IAN for efficient communications.	When a user moves too far away from the IAN that user's communications device must transition to the JAN in a way that is seamless to the user.

8.1.4 Jurisdiction Area Network

This section defines the network performance requirements for the JAN.

8.1.4.1 Performance Metrics

This section defines performance metrics for the JAN.

8.1.4.1.1 Class of Service 0

This section defines performance requirements for the JAN that are specific to Class of Service 0.

Matrix 61: Jurisdiction Area Network Requirements 1

PS SoR Section 8.1.4.1.1 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 0.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 0.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.

Matrix 61: Jurisdiction Area Network Requirements 1 (Continued)

PS SoR Section 8.1.4.1.1 Requirement #	Qualitative Requirement Description	Additional Information
3	A maximum packet loss ratio will be established for this network for Class of Service 0.	This requirement an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 0.	This requirement an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the IAN, JAN, and EAN.

8.1.4.1.2 Class of Service 1

This section defines performance requirements for the JAN that are specific to Class of Service 1.

Matrix 62: Jurisdiction Area Network Requirements 2

PS SoR Section 8.1.4.1.2 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 1.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 1.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 1.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the IAN, JAN, and EAN.

Matrix 62: Jurisdiction Area Network Requirements 2 (Continued)

PS SoR Section 8.1.4.1.2 Requirement #	Qualitative Requirement Description	Additional Information
4	A maximum packet error ratio will be established for this network for Class of Service 1.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the IAN, JAN, and EAN.

8.1.4.1.3 Class of Service 2

This section defines performance requirements for the JAN that are specific to Class of Service 2.

Matrix 63: Jurisdiction Area Network Requirements 3

PS SoR Section 8.1.4.1.3 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 2.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 2.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 2.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 2.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the IAN, JAN, and EAN.

8.1.4.1.4 Class of Service 3

This section defines performance requirements for the JAN that are specific to Class of Service 3.

Matrix 64: Jurisdiction Area Network Requirements 4

PS SoR Section 8.1.4.1.4 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 3.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 3.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 3.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 3.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the IAN, JAN, and EAN.

8.1.4.1.5 Class of Service 4

This section defines performance requirements for the JAN that are specific to Class of Service 4.

Matrix 65: Jurisdiction Area Network Requirements 5

PS SoR Section 8.1.4.1.5 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 4.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.

Matrix 65: Jurisdiction Area Network Requirements 5 (Continued)

PS SoR Section 8.1.4.1.5 Requirement #	Qualitative Requirement Description	Additional Information
2	A maximum packet delay variation will be established for this network for Class of Service 4.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 4.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 4.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the IAN, JAN, and EAN.

8.1.4.1.6 Class of Service 5

This section defines performance requirements for the JAN that are specific to Class of Service 5.

Matrix 66: Jurisdiction Area Network Requirements 6

PS SoR Section 8.1.4.1.6 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 5.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 5.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.

Matrix 66: Jurisdiction Area Network Requirements 6 (Continued)

PS SoR Section 8.1.4.1.6 Requirement #	Qualitative Requirement Description	Additional Information
3	A maximum packet loss ratio will be established for this network for Class of Service 5.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 5.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the IAN, JAN, and EAN.

8.1.4.2 Reliability

This section defines reliability requirements for the JAN.

Matrix 67: Jurisdiction Area Network Requirements 7

PS SoR Section 8.1.4.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must be capable of handling all of the Class of Service 0 traffic, and any signaling associated with it, even under constrained network conditions.	Pre-emption, over-engineering the network, and other methods are all possible solutions to satisfy this requirement.
2	The network must have a minimum defined reliability. Reliability is defined as the percentage of packets delivered that satisfy Class of Service requirements on the first try.	

8.1.4.3 Availability

This section defines the temporal and spatial availability requirements for the JAN.

8.1.4.3.1 Temporal

This section defines the temporal, or time-based requirements for the JAN.

Matrix 68: Jurisdiction Area Network Requirements 8

PS SoR Section 8.1.4.3.1 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must have a defined minimum acceptable temporal availability. Additionally, a clear and cohesive measurement methodology will be defined to address this requirement.	
2	The network must be capable of operating 24 hours a day, 7 days a week, 365 days a year.	

8.1.4.3.2 Spatial

This section defines the spatial, or space-based, requirements for the JAN.

Matrix 69: Jurisdiction Area Network Requirements 9

PS SoR Section 8.1.4.3.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must have a defined minimum acceptable spatial availability. Additionally, a clear and cohesive measurement methodology will be defined to address this requirement.	This requirement will define how many devices must be capable of operating on a single PAN.

8.1.4.4 Scalability

This section defines horizontal and vertical scalability requirements for the JAN.

8.1.4.4.1 Horizontal

This section defines the horizontal, or coverage area, scalability for the JAN.

Matrix 70: Jurisdiction Area Network Requirements 10

PS SoR Section 8.1.4.4.1 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must be able to scale in terms of coverage area in a very cost-efficient manner, while still meeting all of the requirements for the particular type of network that is being extended.	The first responder community will determine the affordability of adding more coverage area through a new base station or repeater; this action will not decrease the performance of the network, regardless of the density of such infrastructure pieces.
2	The network must support the ability to add new infrastructural components into the existing infrastructure and become operational with little to no configuration or setup required.	This requirement defines the concept of the network practicing self discovery of infrastructure devices being added to the network.

8.1.4.4.2 Vertical

This section defines the vertical, or number of users, scalability for the JAN.

Matrix 71: Jurisdiction Area Network Requirements 11

PS SoR Section 8.1.4.4.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must be capable of dynamically scaling to accommodate a growing number of users while not sacrificing any mission-critical services or applications.	This requirement must be adhered to, even in a constrained or congested networking environment.

8.1.4.5 Survivability

This section defines survivability requirements for the JAN. Survivability is the ability of the network to continue operating under adverse or destructive conditions.

Matrix 72: Jurisdiction Area Network Requirements 12

PS SoR Section 8.1.4.5 Requirement #	Qualitative Requirement Description	Additional Information
1	The network will not have any SPOF where economically feasible.	This is an agency-specific requirement calling attention to SPOFs as an engineering reality that must be appropriately weighed and addressed.
2	The network must be capable of self-healing functionality	This can be likened to a routing protocol that entails routing around a failed link
3	The network must support ad hoc network creation in the absence of infrastructure	
4	The network must be able to operate through power fluctuations or power loss for a defined period of time	

8.1.4.6 Restorability

This section defines the restorability requirements of the JAN. Restorability is the ease of restoring JAN functionality in the event of a catastrophic failure.

Matrix 73: Jurisdiction Area Network Requirements 13

PS SoR Section 8.1.4.6 Requirement #	Qualitative Requirement Description	Additional Information
1	The network will have a defined maximum amount of time for restoration or replacement of critical infrastructure.	

8.1.4.7 Spectrum and/or Network Efficiency

This section defines the requirements for spectrum and network efficiency for the JAN.

Matrix 74: Jurisdiction Area Network Requirements 14

PS SoR Section 8.1.4.7 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support multicast communications. Multicast occurs when one device sends data across the network to multiple devices. However, depending on the multicast protocol, only nodes that are on the path from the originating device to the receiving device receive and forward the data.	
2	The network must support efficient, unique, plug-and-play addressing of every object on the network that receives or transmits information of any kind.	
3	The RF system must be spectrally efficient to a minimum quantifiable degree.	
4	The goodput (information-to-overhead ratio) of the network must be specific to a minimum quantifiable degree.	

8.1.4.8 Mobility

This section defines the mobility or roaming requirements for the JAN.

Matrix 75: Jurisdiction Area Network Requirements 15

PS SoR Section 8.1.4.8 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support user motion while traveling at reasonable speeds. A reasonable speed implies speeds up to and including aircraft, such as helicopters or small propeller-driven planes.	

Matrix 75: Jurisdiction Area Network Requirements 15 (Continued)

PS SoR Section 8.1.4.8 Requirement #	Qualitative Requirement Description	Additional Information
2	The network must support user transition across multiple jurisdictions while maintaining constant communications and full user functionality.	This requirement includes the ability to roam from jurisdiction to jurisdiction and maintain communications in any jurisdiction, as defined by local policy.

8.1.5 Extended Area Network

This section defines the network performance requirements for the EAN.

8.1.5.1 Performance Metrics

This section defines performance metrics for the EAN.

8.1.5.1.1 Class of Service 0

This section defines performance requirements for the EAN that are specific to Class of Service 0.

Matrix 76: Extended Area Network Requirements 1

PS SoR Section 8.1.5.1.1 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 0.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the PAN, IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 0.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 0.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the PAN, IAN, JAN, and EAN.

Matrix 76: Extended Area Network Requirements 1 (Continued)

PS SoR Section 8.1.5.1.1 Requirement #	Qualitative Requirement Description	Additional Information
4	A maximum packet error ratio will be established for this network for Class of Service 0.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the PAN, IAN, JAN, and EAN.

8.1.5.1.2 Class of Service 1

This section defines performance requirements for the EAN that are specific to Class of Service 1.

Matrix 77: Extended Area Network Requirements 2

PS SoR Section 8.1.5.1.2 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 1.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the PAN, IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 1.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, the JAN, and the EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 1.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the PAN, IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 1.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the PAN, IAN, JAN, and EAN.

8.1.5.1.3 Class of Service 2

This section defines performance requirements for the EAN that are specific to Class of Service 2.

Matrix 78: Extended Area Network Requirements 3

PS SoR Section 8.1.5.1.3 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 2.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the PAN, IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 2.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 2.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the PAN, IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 2.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the PAN, IAN, JAN, and EAN.

8.1.5.1.4 Class of Service 3

This section defines performance requirements for the EAN that are specific to Class of Service 3.

Matrix 79: Extended Area Network Requirements 4

PS SoR Section 8.1.5.1.4 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 3.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the PAN, IAN, JAN, and EAN.

Matrix 79: Extended Area Network Requirements 4 (Continued)

PS SoR Section 8.1.5.1.4 Requirement #	Qualitative Requirement Description	Additional Information
2	A maximum packet delay variation will be established for this network for Class of Service 3.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 3.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the PAN, IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 3.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the PAN, IAN, JAN, and EAN.

8.1.5.1.5 Class of Service 4

This section defines performance requirements for the EAN that are specific to Class of Service 4.

Matrix 80: Extended Area Network Requirements 5

PS SoR Section 8.1.5.1.5 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 4.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the PAN, IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 4.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.

Matrix 80: Extended Area Network Requirements 5 (Continued)

PS SoR Section 8.1.5.1.5 Requirement #	Qualitative Requirement Description	Additional Information
3	A maximum packet loss ratio will be established for this network for Class of Service 4.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the PAN, IAN, JAN, and EAN.
4	A maximum packet error ratio will be established for this network for Class of Service 4.	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the PAN, IAN, JAN, and EAN.

8.1.5.1.6 Class of Service 5

This section defines performance requirements for the EAN that are specific to Class of Service 5.

Matrix 81: Extended Area Network Requirements 6

PS SoR Section 8.1.5.1.6 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum packet transfer delay will be established for this network for Class of Service 5.	This requirement is an upper bound. This maximum delay will be part of an overall link budget that includes transmission on the PAN, IAN, JAN, and EAN.
2	A maximum packet delay variation will be established for this network for Class of Service 5.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation will be part of an overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum packet loss ratio will be established for this network for Class of Service 5.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio will be part of the overall loss ratio for any communications path, including the PAN, IAN, JAN, and EAN.

Matrix 81: Extended Area Network Requirements 6 (Continued)

PS SoR Section 8.1.5.1.6 Requirement #	Qualitative Requirement Description	Additional Information
4	A maximum packet error ratio will be established for this network for Class of Service 5	This requirement is an upper bound. This maximum error ratio will be part of the overall error ratio for any communications path, including the PAN, IAN, JAN, and EAN.

8.1.5.2 Reliability

This section defines reliability requirements for the EAN.

Matrix 82: Extended Area Network Requirements 7

PS SoR Section 8.1.5.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must be capable of handling all of the Class of Service 0 traffic, and any signaling associated with it, even under constrained network conditions.	Pre-emption, over-engineering the network, and other methods are all possible solutions to satisfy this requirement.
2	The network must have a minimum defined reliability. Reliability is defined as the percentage of packets delivered that satisfy Class of Service requirements on the first try.	

8.1.5.3 Availability

This section defines the temporal and spatial availability requirements for the EAN.

8.1.5.3.1 Temporal

This section defines the temporal, or time-based, requirements for the EAN.

Matrix 83: Extended Area Network Requirements 8

PS SoR Section 8.1.5.3.1 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must have a defined minimum acceptable temporal availability. Additionally, a clear and cohesive measurement methodology will be defined to address this requirement.	
2	The network must be capable of operating 24 hours a day, 7 days a week, 365 days a year.	

8.1.5.3.2 Spatial

This section defines the spatial, or space-based, requirements for the EAN.

Matrix 84: Extended Area Network Requirements 9

PS SoR Section 8.1.5.3.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must have a defined minimum acceptable spatial availability. Additionally, a clear and cohesive measurement methodology will be defined to address this requirement.	This requirement will define how many devices must be capable of operating on a single EAN.

8.1.5.4 Scalability

This section defines horizontal and vertical scalability requirements for the EAN.

8.1.5.4.1 Horizontal

This section defines the horizontal, or coverage area, scalability for the EAN.

Matrix 85: Extended Area Network Requirements 10

PS SoR Section 8.1.5.4.1 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must be able to scale in terms of coverage area in a very cost-efficient manner, while still meeting all of the requirements for the particular type of network that is being extended.	The first responder community will determine the affordability of adding more coverage area through a new base station or repeater; this action will not decrease the performance of the network, regardless of the density of such infrastructure pieces.
2	The network must support the ability to add new infrastructural components into the existing infrastructure and become operational with little to no configuration or setup required.	This requirement defines the concept of the network practicing self discovery of infrastructure devices being added to the network.

8.1.5.4.2 Vertical

This section defines the vertical, or number of users, scalability for the EAN.

Matrix 86: Extended Area Network Requirements 11

PS SoR Section 8.1.5.4.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must be capable of dynamically scaling to accommodate a growing number of users while not sacrificing any mission-critical services or applications.	This requirement must be adhered to, even in a constrained or congested networking environment.

8.1.5.5 Survivability

This section defines survivability requirements for the EAN. Survivability is the ability of the network to continue operating under adverse or destructive conditions.

Matrix 87: Extended Area Network Requirements 12

PS SoR Section 8.1.5.5 Requirement #	Qualitative Requirement Description	Additional Information
1	The network will not have any SPOF where economically feasible.	This is an agency-specific requirement calling attention to SPOFs as an engineering reality that must be appropriately weighed and addressed.
2	The network must be capable of self-healing functionality.	This can be likened to a routing protocol that entails routing around a failed link.
3	The network must support ad hoc network creation in the absence of infrastructure.	
4	The network must be able to operate through power fluctuations or power loss for a defined period of time.	

8.1.5.6 Restorability

This section defines the restorability requirements of the EAN. Restorability is the ease of restoring EAN functionality in the event of a catastrophic failure.

Matrix 88: Extended Area Network Requirements 13

PS SoR Section 8.1.5.6 Requirement #	Qualitative Requirement Description	Additional Information
1	The network will have a defined maximum amount of time for restoration or replacement of critical infrastructure.	

8.1.5.7 Spectrum and/or Network Efficiency

This section defines the requirements for spectrum and/or network efficiency for the EAN.

Matrix 89: Extended Area Network Requirements 14

PS SoR Section 8.1.5.7 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support multicast communications. Multicast occurs when one device sends data across the network to multiple devices. However, depending on the multicast protocol, only nodes that are on the path from the originating device to the receiving device receive and forward the data.	
2	The network must support efficient, unique, plug-and-play addressing of every object on the network that receives and/or transmits information of any kind.	
3	The RF system must be spectrally efficient to a minimum quantifiable degree.	
4	The goodput (information-to-overhead ratio) of the network must be specific to a minimum quantifiable degree.	

8.1.6 End-to-End Service Requirements

8.1.6.1 Performance Metrics

This section defines end-to-end performance metrics. The following is an example of end-to-end communications: one first responder converses with another first responder and the following networks are traversed: IAN → JAN → EAN → JAN → IAN. In these requirements, the complete network traversed must be taken into account.

8.1.6.1.1 Class of Service 0

This section defines end-to-end performance requirements that are specific to Class of Service 0.

Matrix 90: End-to-End Service Requirements 1

PS SoR Section 8.1.6.1.1 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum end-to-end packet transfer delay will be established for Class of Service 0.	This requirement is an upper bound. This maximum delay is the overall link budget that includes transmission on the PAN, IAN, JAN, and EAN.
2	A maximum end-to-end packet delay variation will be established for Class of Service 0.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation is the overall link budget that includes transmission on the Incident Area Network, the Jurisdiction Area Network, and the Extended Area Network.
3	A maximum end-to-end packet loss ratio will be established for Class of Service 0.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio is the overall loss ratio for any communications path, including the Personal Area Network, the IAN, JAN, and EAN.
4	A maximum end-to-end packet error ratio will be established for Class of Service 0.	This requirement is an upper bound. This maximum error ratio is the overall error ratio for any communications path, including the PAN, IAN, JAN, and EAN.

8.1.6.1.2 Class of Service 1

This section defines end-to-end performance requirements that are specific to Class of Service 1.

Matrix 91: End-to-End Service Requirements 2

PS SoR Section 8.1.6.1.2 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum end-to-end packet transfer delay will be established for Class of Service 1.	This requirement is an upper bound. This maximum delay is the overall link budget that includes transmission on the PAN, IAN, JAN, and EAN.

Matrix 91: End-to-End Service Requirements 2 (Continued)

PS SoR Section 8.1.6.1.2 Requirement #	Qualitative Requirement Description	Additional Information
2	A maximum end-to-end packet delay variation will be established for Class of Service 1.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation is the overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum end-to-end packet loss ratio will be established for Class of Service 1.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio is the overall loss ratio for any communications path, including the PAN, IAN, JAN, and EAN.
4	A maximum end-to-end packet error ratio will be established for Class of Service 1.	This requirement is an upper bound. This maximum error ratio is the overall error ratio for any communications path, including the PAN, IAN, JAN, and EAN.

8.1.6.1.3 Class of Service 2

This section defines end-to-end performance requirements that are specific to Class of Service 2.

Matrix 92: End-to-End Service Requirements 3

PS SoR Section 8.1.6.1.3 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum end-to-end packet transfer delay will be established for Class of Service 2.	This requirement is an upper bound. This maximum delay is the overall link budget that includes transmission on the PAN, IAN, JAN, and EAN.
2	A maximum end-to-end packet delay variation will be established for Class of Service 2.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation is the overall link budget that includes transmission on the IAN, JAN, and EAN.

Matrix 92: End-to-End Service Requirements 3 (Continued)

PS SoR Section 8.1.6.1.3 Requirement #	Qualitative Requirement Description	Additional Information
3	A maximum end-to-end packet loss ratio will be established for Class of Service 2.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio is the overall loss ratio for any communications path, including the PAN, IAN, JAN, and EAN.
4	A maximum end-to-end packet error ratio will be established for Class of Service 2.	This requirement is an upper bound. This maximum error ratio is the overall error ratio for any communications path, including the PAN, IAN, JAN, and EAN.

8.1.6.1.4 Class of Service 3

This section defines end-to-end performance requirements that are specific to Class of Service 3.

Matrix 93: End-to-End Service Requirements 4

PS SoR Section 8.1.6.1.4 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum end-to-end packet transfer delay will be established for Class of Service 3.	This requirement is an upper bound. This maximum delay is the overall link budget that includes transmission on the PAN, IAN, JAN, and EAN.
2	A maximum end-to-end packet delay variation will be established for Class of Service 3.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation is the overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum end-to-end packet loss ratio will be established for Class of Service 3.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio is the overall loss ratio for any communications path, including the PAN, IAN, JAN, and EAN.
4	A maximum end-to-end packet error ratio will be established for Class of Service 3.	This requirement is an upper bound. This maximum error ratio is the overall error ratio for any communications path, including the PAN, IAN, JAN, and EAN.

8.1.6.1.5 Class of Service 4

This section defines end-to-end performance requirements that are specific to Class of Service 4.

Matrix 94: End-to-End Service Requirements 5

PS SoR Section 8.1.6.1.5 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum end-to-end packet transfer delay will be established for Class of Service 4.	This requirement is an upper bound. This maximum delay is the overall link budget that includes transmission on the PAN, IAN, JAN, and EAN.
2	A maximum end-to-end packet delay variation will be established for Class of Service 4.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation is the overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum end-to-end packet loss ratio will be established for Class of Service 4.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio is the overall loss ratio for any communications path, including the PAN, IAN, JAN, and EAN.
4	A maximum end-to-end packet error ratio will be established for Class of Service 4.	This requirement is an upper bound. This maximum error ratio is the overall error ratio for any communications path, including the PAN, IAN, JAN, and EAN.

8.1.6.1.6 Class of Service 5

This section defines end-to-end performance requirements that are specific to Class of Service 5.

Matrix 95: End-to-End Service Requirements 6

PS SoR Section 8.1.6.1.6 Requirement #	Qualitative Requirement Description	Additional Information
1	A maximum end-to-end packet transfer delay will be established for Class of Service 5.	This requirement is an upper bound. This maximum delay is the overall link budget that includes transmission on the PAN, IAN, JAN, and EAN.

Matrix 95: End-to-End Service Requirements 6 (Continued)

PS SoR Section 8.1.6.1.6 Requirement #	Qualitative Requirement Description	Additional Information
2	A maximum end-to-end packet delay variation will be established for Class of Service 5.	This requirement is an upper bound on 1 – 10^-3 quantile of packet transfer delay minus the minimum packet transfer delay. This maximum delay variation is the overall link budget that includes transmission on the IAN, JAN, and EAN.
3	A maximum end-to-end packet loss ratio will be established for Class of Service 5.	This requirement is an upper bound on the packet loss probability. This maximum loss ratio is the overall loss ratio for any communications path, including the PAN, IAN, JAN, and EAN.
4	A maximum end-to-end packet error ratio will be established for Class of Service 5.	This requirement is an upper bound. This maximum error ratio is the overall error ratio for any communications path, including the PAN, IAN, JAN, and EAN.

8.2 Interfaces

This section covers the non-public safety networks that will need an interface for sending and/or receiving information from public safety. All of these interfaces will be made through the EAN.

Matrix 96: Interfaces Requirements

PS SoR Section 8.2 Requirement #	Qualitative Requirement Description	Additional Information
1	The network must support the capability to interface with the PSTN.	
2	The network must support interfacing with public utility information, such as for the power grid, natural gas distribution systems, etc.	The level of security needed for this interface needs to be understandably high due to concerns of terrorist attacks on such utilities.
3	The network must support the capability to interface with non-public safety data networks, including the Internet, in a secure manner.	An example service is the IAmAlive service. Other examples include communications with Public Health agencies, Emergency Management Departments, and other pertinent organizations.

Matrix 96: Interfaces Requirements (Continued)

PS SoR Section 8.2 Requirement #	Qualitative Requirement Description	Additional Information
4	The network must be capable of accessing real-time weather information.	Weather information can take the form of a forecast, current weather at a given site, network sensors, etc.
5	The network must support the capability to interface with the Department of Transportation's ITS.	

Appendix A Glossary and Acronyms

A

ACN

Automatic Call Notification

Access control

Both public safety users and public safety user devices must be authenticated before they are given access to network resources.

ACS

American College of Surgeons

AES

Advanced Encryption Standard

APB

All Points Bulletin

ATF

Bureau of Alcohol, Tobacco, Firearms, and Explosives

Attack prevention and detection

Communications networks must be resistant to jamming, capable of passive and active attack monitoring and defense deployment, able to geolocate the source of an attack, and capable of monitoring functional aspects of all authorized user-devices.

Authorization

Once a user has been granted access to the system, the services and information that the user has access to will be determined by that users' authorization level.

AVL

Automatic Vehicle Location

C

C&I

Communications and Interoperability

CAD

Computer Aided Dispatch

CBR&E

Chemical, Biological, Radiological, and Explosive

CDC

Centers for Disease Control and Prevention

CERT

Community Emergency Response Teams: Trained civilian volunteer auxiliary responders that assist victims and provide support for professional responders during a major disaster.

CJIS

Criminal Justice Information System

D

Day-to-day

Routine or day-to-day operations fit a general normal structure for the public safety personnel and should not tax their ability to deal with communications processes and procedures. Many of these operations may be strictly within the discipline or agency with no communications interoperability requirements with other disciplines or agencies at all. However, as described in the PSWAC Final Report, day-to-day operations can include the need for city law enforcement personnel to communicate with their county law enforcement personnel and vice-versa.

The ability to communicate minimizes the need for dispatcher-to-dispatcher interaction in the exchange of information among units in the field.

Day-to-day operations can also include task force operations to carry out a specific mission, such as a DUI (Driving Under the Influence) stake-out, where the communications are within the agency and do not require interoperability with other agencies. Also on a day-to-day basis, an agency (such as one fire district) can provide mutual aid to another agency (a second fire district) while the first agency covers an emergency.

DFFP

Department of Forestry and Fire Protection

DHS

Department of Homeland Security

DMAT
Disaster Medical Assistance Teams: A mobile medical field unit staffed and equipped to treat large numbers of injured.

DMORT
Disaster Mortuary Operational Response Team

DMV
Department of Motor Vehicles

DOB
Date of Birth

DoT
Department of Transportation

DPW
Department of Public Works

E

EAN
See Extended Area Network.

ED
Emergency Department

EKG
Electrocardiogram

EM
Emergency Manager

EMS
Emergency Medical Services

EMT
Emergency Medical Technician

EMT-P
Emergency Medical Technician-Paramedic

EOC
Emergency Operations Center

EOD
Explosive Ordnance Disposal

EMP
Emergency Management Plan

ER
Emergency Room

Extended Area Network
An EAN is a local system linked with county, regional, state, and national systems. This network can be both wired and wireless, depending on the type of infrastructure deployed in the area (i.e., microwave point-to-point, fiber, etc.).

F

FBI
Federal Bureau of Investigation

FCC
Federal Communications Commission

FD
Fire Department

FEMA
Federal Emergency Management Agency

FIMO
Federal Incident Manager Official

FIPS
Federal Information Processing Standard

FLIR
Forward Looking Infrared

FRV
First Responder Vehicle

G

GHz
Gigahertz

GIS
Global Information System

H

Hazmat
Hazardous Materials

HIPAA
Health Insurance Portability and Accountability Act

I

IAN
See Incident Area Network.

IC
Incident Command or Incident Commander

ICS

Incident Command System

Incident command structure

An incident command structure supports the need for The communications systems that must support the agency's incident command policies.

Incident Area Network

An IAN is a network created for a specific incident. This network is temporary in nature and is typically centered on a wireless access point attached to the first responders' vehicle, or IAN nodes. Multiple vehicles therefore dictate multiple IAN nodes, all of which coordinate their coverage and transmissions seamlessly and automatically. This network scales to the size of the incident, from a local traffic stop, to a large-scale, multi-discipline, multi-jurisdiction event.

Integrity

Integrity refers to the requirement The communications systems must not allow undetectable modification of traffic while in transit.

Interactive data communications

These communications will provide practitioners with maps, floor plans, video scenes, etc., during an emergency. In the context of the type of communications, interactive means that there is a query made and a response provided. The query and response need not be initiated by a practitioner and can include automated queries/responses. Commanders, supervisors, medical staff, etc., can make more intelligent decisions more efficiently with data from field personnel. Similarly, personnel entering a burning building armed with information about the building, such as contents, locations of stairwells, hallways, etc., can also perform their duties better.

Interactive voice communications

Interactive voice communications involve the reality that communications between public safety practitioners and their supervisors, dispatchers, members of the task force, etc., that require immediate and high-quality response, with much higher performance demands than those required by commercial users of wireless communications. Commands, instructions, advice, and information are exchanged that often result in life and health benefit situations for public safety practitioners, as well as for the public.

IP

Internet Protocol

IPR

Intellectual Property Rights

IR

Infrared

IST-Incident Support Team

Supports US&R teams with tasking, material, and coordination. US&R teams are task forces equipped with the necessary tools and equipment and the required skills and techniques for the search, rescue, and medical care of victims of structural collapse.

ITS

Department of Transportation: Intelligent Transportation System

National Telecommunications and Information Administration: Institute for Telecommunications Sciences

J

JAN

See Jurisdiction Area Network.

JIC

Joint Information Center

JTTF

Joint Terrorism Task Force

Jurisdiction Area Network

The JAN is the main communications network for first responders. It is responsible for all non-IAN voice and data traffic. It handles any IAN traffic that needs access to the general network, as well as providing the connectivity to the EAN. Additionally, it is the component of the network that will handle any and all communications from a first responder PSCD should a connection with the local IAN fail or be otherwise unavailable.

L

LAN
local area network

LE
Law Enforcement

LMR
Land Mobile Radio

M

MCC
Mobile Commander Center

Medical communications system
A database containing information on the real-time status of emergency medical personnel, resources, hospitals, and patients that is accessible by command personnel, authorized responders, health care facilities, etc.

MERS
Mobile Emergency Response System

MHz
Megahertz

MSO
Mobile Switching Office

Multicast
Instance when one device sends data across the network to multiple devices; however, depending on the multicast protocol, only nodes that are on the path from the originating device to the receiving device receive and forward the data.

Mutual aid
Mode describing those major events with large numbers of agencies involved, including agencies from remote locations. Their communications are not usually well planned or rehearsed. The communications must allow the individual agencies carry out their missions at the event, but follow the command and control structure appropriate to coordinate the many agencies involved with the event.

N

NAWAS
National Warning System

NCIC
National Crime Information Center

NIJ
National Institute of Justice

NIMS
National Incident Management System

NIRSC
National Incident Radio Support Cache

NIST
National Institute for Standards and Technology

Non-interactive data communications
A one-way stream of data, such as the monitoring of firefighter biometrics and location, that greatly increases the safety of the practitioners. This form of communications also makes meeting the command and control requirements easier because the commander is aware of the condition and location of the on-scene personnel.

Non-interactive voice communications
These communications occur when a dispatcher or supervisor alerts members of a group about emergency situations to share information. In many cases, the non-interactive voice communications have the same mission-critical needs as the interactive service.

NTIA
National Telecommunications and Information Administration

O

OEM
Office of Emergency Management

P

PABX
Private Automatic Branch Exchange

PAN
See Personal Area Network.

Personal Area Network
The PAN for a first responder can take many forms. Primarily, it is intended to represent a set of devices on the person of a first responder that

communicate with the first responder's PSCD as necessary. The devices on a PAN will include such items as heart rate monitors, location sensors, etc. Information from these devices could, and would in many cases, be transmitted to other areas of the network.

PIO

Public Information Officer

PPC

Prevention Preparedness Council

Privacy

The communications systems must allow only intended and authorized recipients to see information as well as follow national and state policies (e.g., Health Insurance Portability and Accountability Act-HIPAA).

PSAF

Public Safety Architecture Framework

PSAP

Public Safety Answering Point: The answering center for 911 calls.

PSCD

Public Safety Communications Device. Public safety personnel in the scenarios described in this document communicate using a device that is portable (handheld or wearable), unless specifically noted for command post or other in-vehicle use. Throughout this document, these devices are referred to as Public Safety Communications Devices (PSCD). These devices perform the communications functionality as defined in the scenario. Because these scenarios emphasize communications capabilities, other important considerations for technology development, such as form (e.g., how text data is input to the device via keyboard, stylus, or spoken language) are not discussed. The scenarios also do not distinguish whether a public safety individual is carrying one or more such devices; however, it is noted that minimizing the number of separate devices required to provide the described functionality is preferred, consistent with other requirements, such as affordability and maintainability.

PS SoR

Public Safety Statement of Requirements

PSTN

Public Switched Telephone Network. The public telephone system.

PSWAC

Public Safety Wireless Advisory Committee

Personal Area Network (PAN)

The PAN for a first responder in this document can take on many different forms. Primarily, it is intended to represent a set of wired devices on the person of a first responder, whose data is aggregated out of a transceiver to the first responders' PSCD. The devices on a PAN will include such things as heart rate monitors, location sensors, etc.

R

RACES

Radio Amateur Civil Emergency Service

Reverse 911

REVERSE 911 is a Microsoft Windows-based program that uses a combination of database and GIS technologies that can target a precise geographic area and saturate it with thousands of calls per hour. The software can also create a list of individuals with common characteristics (such as a Neighborhood Crime Watch group or emergency personnel) and contact them rapidly whenever necessary.

RFID

Radio Frequency Identification

RMS

Records Management System

S

S&T

Science & Technology Directorate (DHS)

SAC

Special Agent in Charge

SHA

Secure Hash Algorithm

SoR

Statement of Requirements

SPOF

Single Points of Failure

System administration of users

The communications systems must allow authorized system administrators, as well as incident and branch commanders, to establish user profiles for network access and usage, depending on the role that the public safety user is asked to satisfy during an incident.

T

Task force

Mode that defines a cooperative effort between specific agencies with extensive pre-planning and practice of the operation. As the PSWAC Final Report indicates, the communications tends to be at close range and the traffic requires rapid or immediate response times. In today's environment, task forces, such as a terrorism task force, may cover a broad regional area and not operate exclusively at close range. These operations present additional challenges.

Temporary network

JANs and EANs are networks that exist at all times whereas the IANs are created on temporary basis to serve a particular purpose, such as an incident and then are dissolved. The nature of the IAN is such that it may not reach all areas of an incident. In such cases, the user would either connect to the JAN, or create a temporary network to extend the IAN to the area not covered.

TSA

Transportation Security Administration

U

US&R

Urban Search and Rescue. A task force equipped with necessary tools and equipment and the required skills and techniques for the search, rescue, and medical care of victims of structural collapse.

User/User group

Public safety personnel and resources that are recognized by the system to share communications and information. This implies that traffic related to this user group only traverses the portion of the network necessary to reach all members of particular user group. Each user group can be a permanent unit or a temporary unit created by an authorized user for a particular task.

User identification and location

The communications systems must provide user identification to others during communications and when required, must provide user geolocation information to incident commanders and other authorized resources.

V

VHF

Very High Frequency

Video Teleconferencing

Video teleconferencing, in the context of this document, refers to video directly coupled with audio in a fully interactive two-way session. Other terms used include multimedia and video conferencing.

VMS

Variable Message Signs

VSAT

Very Small Aperture Terminal

Appendix B SAFECOM-AGILE-NIST/OLES Summit

SAFECOM-AGILE-NIST Summit on Interoperable Communications for Public Safety

The Summit on Interoperable Communications for Public Safety, held at the National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland, on June 26 and 27, 2003, was a joint effort among NIST, the Department of Homeland Security's Science and Technology (S&T) Directorate, the SAFECOM Program, and the National Institute of Justice's Advanced Generation of Interoperability for Law Enforcement (AGILE) Program. The summit brought together a variety of programs that were created to assist public safety practitioners, including first responders.

This summit was restricted to Federal agencies and national, state, and local organizations with responsibility for first-responder communications.

The summit was the initial step in familiarizing key interoperability players with the work being done by others to establish mutually beneficial coordination and collaboration among the various technical programs. The summit also provided insight into where additional Federal resources might be warranted, and has helped stakeholders maximize the limited resources that are available across all government levels by leveraging program successes and developing standards, approaches, products, and services for the benefit of all.

The information resulting from the summit may prove to be significant in helping to formulate a coordinated approach or approaches toward nationwide communications interoperability. Some of the information developed in the summit included a list of system capabilities that participants considered essential for wireless voice, wireless data, and information systems. The List of System Capabilities is in the following sections.

B.1 Wireless Voice Capabilities

Communications Regardless of Technologies, Infrastructures, and Frequency Bands

Ability for users to transparently communicate, as authorized, among multiple agencies/jurisdictions, some of which may use different technologies, infrastructures and/or frequency bands regardless of system. Includes the transitioning between commercial systems and private land mobile radio (LMR) systems.

1. Communication with Own Jurisdiction

   Ability to communicate with members of own agency/jurisdiction while using the infrastructure of another agency/jurisdiction.

2. Communication with Other Jurisdictions

   Ability to communicate with other agencies/jurisdictions using the infrastructure of that agency/jurisdiction.

3. One-to-One Communications

   Ability for users to transparently communicate, as authorized, with members of other agencies/jurisdictions on a unit-to-unit (one-to-one) basis.

4. One-to-Many Communications

   Ability for users to transparently communicate, as authorized, with members of other agencies/jurisdictions on a unit-to-group (one-to-many) basis.

5. Communications Outside Wireless Infrastructure Coverage

   Ability to provide direct communications (talk around) between user radios where wireless infrastructure is unable to support communications (such as in some rural areas, underground parking garages, tunnels, and inside some buildings).

6. Jurisdictional Signal Coverage

   Ability to provide jurisdictional-wide signal coverage to system users; optionally, provide ways to enhance or improve jurisdictional coverage in rural areas, underground parking garages, tunnels, and inside buildings that are usually not sufficiently covered.

7. Identification and Authorization

   Ability to initiate wireless voice communications by requiring the user to enter (on his/her radio) a user identification that authenticates and validates the user and loads the user's profile. This profile defines talk groups for the user and completes all radio network administration for the user's voice communications with other members of the user's agency/jurisdiction and with other agencies/jurisdictions, as authorized.

8. Priority Levels for Access and System Use

   Ability of the agency/jurisdiction to administer the priority for voice communications of particular users and particular public safety applications (such as task force operations and incidents).

9. Emergency Voice Communication

   Ability to communicate an emergency voice message (e.g. after pressing a panic button) that has priority over other voice communications.

10. Emergency Signal

    Ability to broadcast an emergency signal (e.g. via a panic button) that has priority over other communications.

11. Secure Communications

    Ability to have secure (encrypted) voice communications to fit user environment and that satisfy applicable laws, regulations, and policies of the user agencies and jurisdictions.

12. System Administration

    Ability to effectively initiate and sustain flexible and dynamic system administration for purposes of multi-agency interoperability, including administration of talk groups, encryption key management, emergency alerts, networks, and channels for mutual aid.

13. Remotely Reprogram User Radios

    Ability to remotely (over-the-air) re-program a radio's parameters (i.e., frequency channels, talk groups, squelch control, encryption keys, etc.) and/or modify functionality (e.g., encryption algorithms, waveforms, etc.)

14. Resilient Operations

    Ability to sustain resilient operations including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc.

15. Reliable System Performance

    Ability to maintain reliable system performance over disparate interconnected systems.

B.2 Wireless Data Capabilities

1. On-Scene Wireless Data Networks

   Ability to quickly and transparently establish and maintain on-scene wireless data networks (e.g., on scene in a building).

2. On-scene Exchange of Data

   Ability of on-scene personnel to transparently exchange data.

3. High-Speed Data Transfer

   Capability of high-speed data transfer with ability to sustain performance at network interconnections.

4. Communication with Own Jurisdiction

   Ability to exchange data with members of own agency/jurisdiction while using the infrastructure of another agency/jurisdiction.

5. Communication with Other Jurisdictions

   Ability to exchange data with members of other agencies/jurisdictions using the infrastructure of that agency/jurisdiction.

6. Sensor Networks

   Ability to exchange data involving sensors (e.g., biometric, environmental, personnel location).

7. Identification and Authorization

   Ability to initiate wireless data communications by requiring the user to enter (on his/her terminal/radio) a user identification that authenticates and validates the user and loads the user's profile. This profile defines data resource capabilities for the user and completes all radio network administration for the user’s data communications with other members of the user’s agency/jurisdiction and with other agencies/jurisdictions, as previously authorized.

8. System Administration

   Flexible and dynamic system administration (includes administration of wireless data networks, adding users, giving permissions, etc.).

9. Data Security

   Ability to ensure secure exchange of information.

10. Information Protection

    Ability to protect information according to applicable laws and statutes.

11. Resilient Operations

    Ability to sustain resilient operations, including tolerance to individual system failures, redundant coverage from adjacent sites, resistance to impact of catastrophic events, etc.

12. Reliable System Performance

    Ability to maintain reliable system performance over disparate interconnected systems.

B.3 Information Systems Capabilities

1. Rapid Information Source Access

   Ability to provide the exchange of information in a timely fashion to support critical decision points from both field and base locations, including, but not limited to, information regarding identification (photographs, fingerprints, etc.) and activity (criminal history, wants/warrants, reporting/contact history, computer-aided dispatch (CAD) information, building diagrams, building sensors, transportation information, etc.).

2. Query/Access Multiple Data Sources with One Request

   Ability to query/access multiple data sources using one request that is routed to multiple entities simultaneously.

3. "Enter Once—Reuse Forever" Approach to Data Gathering

   Ability to enter validated information once and then share and reuse that information among authorized entities.

4. Data Exchange with Computer-Aided Dispatch

   Ability to exchange information with CAD and Record Management Systems (RMS).

5. Data Access to Logistical Resource Information

   Capability to obtain logistical resource information on all personnel and equipment responding to an incident.

6. Emergency Notifications

   Ability to broadcast critical information by means such as text messaging to multiple organizations

7. Formatting

   Ability to effectively and efficiently exchange data between agencies/jurisdictions (e.g., by employing common data representation structures and exchange formats and protocols).

8. Open Source Formatting

   Ability to effectively and efficiently exchange data between agencies/jurisdictions, e.g., by encouraging open source format.

9. Data Security

   Capability of maintaining the security requirements of any entity within a broader security framework.

10. Field Image Capture and Distribution

    Capability of field image capture and distribution.

11. Data Access to Background Information Sources

    Ability to access information related to hazardous materials, water sources, floor and building plans, fire pre-plans, utility maps, weather forecasts, topographic terrain, transportation, and other background data to support public safety incident management.

12. Data Access to Medical Information

    Ability to manage medical information.

13. Data Access to Legal Information

    Ability to access legal information, such as investigation/litigation records, court scheduling records, disposition data, and charge data.

This page intentionally left blank.

Appendix C Operational Scenarios

This section includes operational scenarios that provide a view of future public safety communications. These scenarios describe credible, realistic incidents, activities, and responses that involve public safety agencies and personnel. While recognizing that this collection does not cover an infinite number of possible activities and situations, they do provide a comprehensive vision of the future of public safety communications.

The scenarios in this section are designed to demonstrate increasingly complex situations. The first two scenarios reflect the interaction of multiple services in a local area:

- A pre-planned event (college football game)

  (See Section C.1.)
- A terrorist car bomb

  (See Section C.2.)

The last two scenarios represent large-scale regional events:

- A hurricane

  (See Section C.3.)
- An earthquake

  (See Section C.4.)

As the scenarios become more complex, details are assumed, and not explicitly defined in the scenario. Each scenario begins with an Outline of the hypothetical event, followed by the Narrative, which explains in detail the events of the scenario in chronological order with time stamps. The focus is on those aspects of the scenarios that affect communications; activities that do not affect communications are not described, or are described only briefly. The Narrative is followed by a Transmission History table, which describes step-by-step the communication events that occur during the scenario.

The level of detail included in the Transmission History table varies, based on the level of detail of the scenario itself, but it generally includes a list of all of the types of communications occurring during the scenario. In many cases, the information in the Transmission Tables describes the creation or dissolution of a user group. While active, there are numerous individual transmissions that are not enumerated; rather, a relative measure of the amount of traffic is provided, from low to very high, to indicate the relative loading the transmissions place on the communications infrastructure.

C.1 Scenario: College Football Game

C.1.1 Outline

Preplanning

1. Columbia State Police (CSP) provide escort for Metropolis football team from its hotel in Harvest Junction.
2. Initial traffic detail deployed.
3. CSP escort meets Central City Police Department (CCPD) escort at city line.
4. Traffic backs up off I-107 due to disabled vehicle; alternative routing established.
5. Traffic detail notices a car fire; fire department responds.
6. 6.Rain begins to freeze in some areas, so Department of Public Works (DPW) is notified and adjusts its priorities to salt areas where traffic is initially most affected.
7. Private citizen calls 911 with parking complaint; unit sent to investigate and calls for tow truck.
8. Patient with chest pains removed from stadium.
9. Officers apprehend a suspect who has broken into a car parked in the parking lot.
10. A12-year-old boy is separated from his family while taking a shuttle bus back to a satellite parking area; police find him in a different parking lot.
11. Traffic detail completed.

C.1.2 Narrative

This scenario outlines the activities associated with a college football game between Columbia State University (CSU) and its archival, Metropolis University, taking place at McDonald Stadium on the campus of CSU in Central City on a gray, chilly November evening.

Several Days Prior

1. The CCPD officer assigned to coordinate the traffic detail contacts the CSU Parking Bureau to coordinate placement of “No Parking” barrels and other details of the upcoming game. The officer also contacts a towing company to provide a tow truck at the Command Post during the game, and contacts the Central City DPW to inform it of the anticipated traffic during game day.

3:45 PM

2. The CSP begin escorting the Metropolis University football team from the Holiday Inn in Harvest Junction to McDonald Stadium. CSP provides escort to the Central City line.

4:00 PM

3. The Command Post at McDonald Stadium is activated, and the officers assigned to traffic detail are assigned to their posts. At key intersections, the officers park their cars to allow cameras in the cars to take video of the traffic situation, which is made available to Incident Command upon request. Officers on traffic detail are placed in a user group with the Command Post. Officers inside the stadium are part of a separate user group with the Command Post as well. The location assignments of the officers are displayed in an overlay on a map display in the Command Center.

4:15 PM

4. The CSP escort approaches the City Line. A user group linking the CSP escort and CCPD escort is established when the CSP escort is about 5 minutes from the handoff point. After the CCPD begins the escort, this user group is dissolved.

5:30 PM

5. Officers on traffic detail at two interchanges along I-107 begin to report in that traffic is backing up along I-107. The commander of the traffic detail checks a monitor in the Command Post and brings up a video display from each of the police cars deployed along the interstate. She also hears a dispatch from the 911 Center that there is a disabled vehicle on I-107. She brings up a video feed from a news station traffic camera mounted on the Highland Park Building. She queries real-time information from the Department of Transportation (DoT) sensor grid to confirm the location of traffic tie-up, and the traffic patterns on side streets. This information is displayed as an overlay to a map display. She creates a temporary user group to link the officers on traffic detail in the affected area, and officers begin to route traffic heading for the game to exit the interstate further north. The Traffic Detail Commander also sends a message to update variable message signs along the interstate to inform motorists of the detour, and sends a message to the DoT Traffic Control Center to change the traffic signal pattern along the alternative route. The commander then periodically brings up the various feeds to monitor how well the rerouting is working.

6:15 PM

6. Officers directing traffic into a parking lot notice flames inside a parked car. They contact the traffic detail commander who contacts the 911 center. A user group is established between the responding fire truck and the traffic detail officers in that parking lot. The traffic detail commander also reassigns some traffic detail officers in the area to assist in clearing a path for the fire truck to reach the vehicle in the parking lot. The fire is quickly extinguished. The traffic detail commander contacts University security inside the stadium to page for the car's owner.

6:30 PM

7. A light mist begins falling and freezing on the road surface. Cars using the alternate routing from I-107 must go up a steep hill to get to McDonald Stadium, and cars are beginning to slide. A traffic detail officer reports the conditions to the traffic detail commander, who contacts the DPW, which reassigns a salt truck to the area. A user group is set up between the traffic detail officer and the salt truck operator to allow the officer to hold up traffic and allow the truck operator to salt the hill unimpeded.

7:00 PM

8. The 911 Center receives a call that a car is blocking a private driveway near the stadium. The dispatcher informs the traffic detail commander, who dispatches a unit to handle the parking complaint. The officer runs a plate check to identify the owner; this information is automatically put into the towing report. The officer then contacts the impound post which dispatches an on-call tow truck to tow the car.

7:15 PM

9. A woman approaches an officer inside the stadium and tells him that her husband is having chest pains. The officer contacts via his PSCD the emergency medical personnel inside the stadium. Medical personnel come to the section where the man is sitting; they quickly conclude the man's symptoms warrant further attention, and contact via PSCD the on-duty physician at the stadium medical station. The physician directs the medical personnel to move the man to the medical station, where an ambulance is located. There the physician concludes that the man should be transported to the Cardiac Care Center at Faith Hospital. The physician contacts the hospital to notify it of the incoming patient. The patient is then placed in the ambulance and transported to the

Cardiac Care Center (following similar procedures as described in the EMS scenario.) As the ambulance leaves the stadium, the Commander informs the traffic detail officers outside the stadium who direct traffic to allow the ambulance quick departure to the hospital.

8:15 PM

10. Officers in their patrol cars periodically download real-time video from surveillance cameras deployed around the parking lots. One officer observes a young male pulling something through the window of a car and then running away. This information is broadcast to the traffic detail users group, and officers on the far side of the lot chase and catch the suspect. The arresting officer requests a transport vehicle to take the suspect to the city jail and completes an arrest report (similar to the procedures described in the Traffic Stop scenario).

10:00 PM

11. As the game ends, city transit buses, which are connected to a user group for all traffic units, shuttle people back to satellite parking areas. As one family arrives at the satellite parking area, they inform a traffic detail officer that they have been separated from their 12-year-old son. The traffic detail officer obtains a photograph of the boy from the mother and captures the image electronically (via scanner or camera). The officer broadcasts the information to the traffic detail officers and the transit bus drivers, and forwards the picture of the boy to the traffic detail officers and transit buses on the users group. One bus driver indicates that he had a passenger that may have fit that description and who left his bus at a particular lot. The traffic detail officers at that lot identify the boy in the crowd from his picture and reunite him with his family. The buses are removed from the traffic users group.

11:30 PM

12. The Metropolis University team is escorted from the stadium. Shortly thereafter, the traffic detail is completed and the user groups are dissolved. CSU wins, 27-21.

C.1.3 Transmission History

There are various specific transmissions in the following table, such as acknowledgements and notifications, that are assumed in the narrative section. Security indicates whether the transmission is secured (S) or unsecured (U). Many of the transmissions described in the narrative occur over the identified user group. In addition, there are “routine” communications on this network that the table does not identify explicitly. In some cases, specific transmissions are identified here to help illustrate the logical flow of events.

Table 31: Transmission History College Football Game Scenario

Time: **ID:**	**Response: LE, Other:**	**Transmission Type and Net Utilization:** **Security:**
Time: 16:00 ID: c1	LE: User group established among officers assigned to traffic detail and the event Command Post	Transmission Type and Net Utilization: Voice/Low Security: U
Time: 16:00 ID: c2	LE: User group established among officers assigned to stadium detail University security, on-site medical personnel, and the event Command Post	Transmission Type and Net Utilization: Voice/Low Security: U

Table 31: Transmission History College Football Game Scenario (Continued)

Time: ID:	Response: LE, Other:	Transmission Type and Net Utilization: Security:
Time: 16:00 ID: c3	LE: Location of traffic detail cars sent to event Command Post and displayed on map	Transmission Type and Net Utilization: Voice/Low Security: U
Time: 16:15 ID: d1	LE: User group established between CSP and Central CCPD escorts	Transmission Type and Net Utilization: Voice/Medium Security: U
Time: 16:20 ID: d2	LE: User group dissolved between CSP and Central CCPD escorts	Transmission Type and Net Utilization: Voice/Medium Security: U
Time: 17:30 ID: e1	LE: Traffic detail commander downloads video from cameras of police cars at intersections	Transmission Type and Net Utilization: Video Security: U
Time: 17:30 ID: e2	LE: Traffic detail commander downloads video from news station traffic camera	Transmission Type and Net Utilization: Video Security: U
Time: 17:30 ID: e3	LE: Traffic detail commander downloads data from DoT sensors	Transmission Type and Net Utilization: Binary Security: U
Time: 17:30 ID: e4	LE: User group established among event Command Post and traffic detail officers in areas where traffic is backed up	Transmission Type and Net Utilization: Binary Security: U
Time: 17:30 ID: e5	LE: Traffic detail commander sends messages to DoT to update variable message signs (VMS) and traffic signal pattern to accommodate re-routed traffic	Transmission Type and Net Utilization: Binary Security: U
Time: 18:15 ID: f1	LE: Traffic detail commander contacts 911 Center regarding car fire Other: 911 dispatches fire truck	Transmission Type and Net Utilization: Voice Security: U
Time: 18:15 ID: f2	LE: User group established between traffic detail and responding fire truck	Transmission Type and Net Utilization: Voice/Medium Security: U
Time: 18:25 ID: f3	LE: Fire truck arrives on scene, extinguishes fire; user group dissolved	Transmission Type and Net Utilization: Voice Security: U
Time: 18:30 ID: g1	LE: Traffic detail commander contacts DPW regarding hazardous road situation	Transmission Type and Net Utilization: Voice Security: U
Time: 18:30 ID: g2	LE: User Group is set up, and links to the traffic detail; network dissolved when truck arrives in area a few minutes later	Transmission Type and Net Utilization: Voice Security: U
Time: 19:00 ID: h1	Other: Citizen call comes into 911 center complaining of illegally parked car blocking driveway; dispatch notifies event Command Post	Transmission Type and Net Utilization: Voice Security: U

Table 31: Transmission History College Football Game Scenario (Continued)

Time: ID:	Response: LE, Other:	Transmission Type and Net Utilization: Security:
Time: 19:00 ID: h2	LE: Event Commander assigns traffic detail unit to handle complaint	Transmission Type and Net Utilization: Voice Security: U
Time: 19:05 ID: h3	LE: Traffic detail officer runs license plate check to identify owner	Transmission Type and Net Utilization: Voice Security: U
Time: 19:05 ID: h4	LE: Officer contacts impound post	Transmission Type and Net Utilization: Voice Security: U
Time: 19:05 ID: h5	LE: Impound post notifies on-call tow truck	Transmission Type and Net Utilization: Voice Security: U
Time: 19:05 ID: h6	LE: Officer generates towing report and submits it to supervisor	Transmission Type and Net Utilization: Binary Security: S
Time: 19:05 ID: i1	LE: Officer communicates with EMS in stadium regarding potential heart attack victim	Transmission Type and Net Utilization: Voice Security: U
Time: 19:05 ID: i2	Other: Medical personnel contact the on-duty physician at the stadium medical station	Transmission Type and Net Utilization: Voice Security: U
Time: 19:05 ID: i3	Other: Physician contacts Cardiac Care Center and updates patient status	Transmission Type and Net Utilization: Voice, Binary Security: U
Time: 19:05 ID: i4	LE: Event commander notifies traffic detail that ambulance is leaving stadium; traffic detail directs traffic accordingly	Transmission Type and Net Utilization: Voice Security: U
Time: 20:15 ID: j1	LE: Officer downloads video from surveillance camera	Transmission Type and Net Utilization: Video Security: U
Time: 20:15 ID: j2	LE: Officer broadcasts alert to traffic detail net	Transmission Type and Net Utilization: Voice Security: U
Time: 22:00 ID: k1	LE: Parents inform traffic detail officer that child is missing; officer captures image of child and sends to other traffic detail officers	Transmission Type and Net Utilization: Image Security: S
Time: 22:00 ID: k2	LE: Temporary net linking traffic detail officers and shuttle bus drivers set up and information about missing boy is broadcast	Transmission Type and Net Utilization: Voice Security: U
Time: 22:00 ID: k3	LE: Bus driver responds on temporary net about passenger who might fit description	Transmission Type and Net Utilization: Voice Security: U
Time: 22:10 ID: k4	LE: Traffic detail officer in identified parking area locates boy based on photograph and bus driver information; temporary net dissolved	Transmission Type and Net Utilization: Voice Security: U
Time: 22:30 ID: l1	LE: Detail completed and all temporary nets dissolved	

C.2 Scenario: Terrorist Car Bomb

C.2.1 Outline

1. An explosion occurs on a downtown street. Numerous calls are received by the Public Safety Answering Point (PSAP). Police, fire, and EMS are dispatched to scene.
2. Police arrive on scene, and Incident Command (IC) is established. A process is initiated to automatically update the roster of on-scene responders using geolocation capabilities with the communications devices and a means for responders to "log in." The police arriving on the scene establish a perimeter by blocking intersections, and clear the area of non-responder individuals and witnesses.
3. Explosive Ordinance Disposal (EOD) unit arrives at the scene and performs a chemical, biological, radiological, and explosives (CBR&E) sweep of area. Ambulances and fire trucks arrive.
4. IC structure evolves to a unified command structure, including a Joint Information Center (JIC).
5. Mass casualty alert is issued, and additional ambulances are dispatched.
6. EOD completes its CBR&E sweep.
7. Fire units begin attacking the fires.
8. EMS triage officers begin tagging bodies.
9. Police begin interviewing witnesses that have been moved into a witness area. Investigation begins; conclusion is reached that explosion caused by car bomb; surveillance video identifies vehicle.
10. Emergency Operations Center (EOC) becomes active and contacts public works and utilities.
11. Ambulances begin transporting patients to hospitals.
12. State troopers are assigned to secure other areas in city.
13. Additional law enforcement support arrives, and police begin to evacuate other buildings in the area. Perimeter control user group is divided.
14. Police and firefighters assist people evacuating buildings.
15. A user group suffers communications performance problems; the communications officer assigns different frequencies to the net.
16. Investigators identify high probability that bomb was planted by terrorist group and identify suspects.
17. An all points bulletin (APB) on suspected perpetrators is issued, and roadblocks are set up. Investigators broadcast a picture of suspects to officers in region and to transportation sites.
18. Ambulances complete transport of victims to hospitals.
19. Officers identify and apprehend a suspect at airport and obtain warrants for suspected accomplices.
20. Electronic case file is prepared, and warrants are requested from judge.
21. Building evacuations are completed. Police officers from outside agencies are released.
22. Evidence technicians begin collecting evidence at the site.

23. A fire in the First National Bank building is extinguished, and fire trucks return to station.

24. LE command is moved to a vacant storefront as investigation continues.

C.2.2 Narrative

Electronic communications between all of the personnel involved in this incident are authenticated. For local on-duty personnel, this authentication takes place when each PSCD is initially logged on. For personnel responding from other local, state, and Federal jurisdictions, the authentication takes place at the time the unit initially joins the incident, and as different databases are queried or additional communications links established. Responders equipped with PSCDs that do not support automatic authentication and registration report to the staging area. Information on the real-time status of emergency medical personnel, resources, hospitals, and patients is contained in a database accessible by command personnel, authorized responders, health care facilities, etc.

5:00 PM

1. An explosion rocks the downtown area of Central City just as rush hour is beginning. The explosion is on Y Street near 20th Street, outside the First National Bank building. The explosion destroys several cars in the immediate vicinity, blows out the glass doors of the bank building, and starts fires in the bank lobby. Numerous calls are immediately placed to the 911 Center. A number of the calls come from wireless devices; location information accompanying the calls allows the dispatchers to quickly identify the area affected by the incident. There are more than 50 victims in the street and in the entryway to the bank, fires have ignited, and there may be structural damage to the bank building. The dispatcher initiates first response of the CCPD, Central City Fire Department (CCFD), and EMS Central City, a contract EMS service. In addition, dispatch requests the EMS mass casualty supplies that are cooperatively stored at Fire Station Number 2, be brought to the scene. Dispatch also contacts the Liberty County Emergency Manager, who authorizes activation of the emergency notification network to alert the county emergency management team.

5:05 PM

2. Within minutes, the first LE personnel arrive on the scene. Because police headquarters is located on X Street and 20th, a number of police officers who heard the explosion, including the Assistant Chief of Police, run to the scene. The Assistant Chief assumes IC for the initial response. He observes the scene and identifies the possibility that the explosion was caused by a car bomb. He immediately requests dispatch of an EOD team.

   A roster of officers on the scene is quickly compiled by electronically querying PSCDs for location information. The IC then organizes several teams to clear the area of bystanders and establish an outer perimeter that extends two blocks in each direction from the bomb scene. Entry through the outer perimeter is permitted only for authorized first responder personnel, and only after the Safety Officer confirms that the area is safe. As additional LE officers approach the area, their PSCDs automatically provide their status on the network. Where feasible, the IC assigns tasks to officers responding to the incident. Several user groups are created—one is set up for officers working the outer perimeter, one for officers clearing the immediate area.

3. An inner perimeter around the immediate blast damage area is established. The Liberty County Sheriff's Office (LCSO) and the area is established between the CSP. The CSP helicopter, with its stabilized platform video camera, is also requested.

4. Shortly thereafter, the first ambulances and fire trucks arrive at the outer perimeter. The first EMT-P on the scene assumes the role of Medical Scene Commander. However, entry into the inner perimeter is delayed until the area is determined to be safe.

5:15 PM

5. The police officers on the scene continue to clear the area of bystanders, "walking wounded," and people attempting to evacuate the area, and anyone other than authorized responders and victims that cannot move. Witnesses are moved to an area for later interviews. They clear a corridor to allow the arriving EOD team to conduct a CBR&E sweep of the area.[6] While the CBR&E sweep is underway, video from a camera mounted on one of the police cars that is responding to the explosion is transmitted to the dispatch center and supervisory offices in the fire and police departments. The video is also transmitted to the fire battalion chief, who is being driven to the scene. Arriving EMTs begin assisting injured people who are able to walk from the scene and reach the perimeter.

5:20 PM

6. When the Fire Battalion Chief arrives, a unified command structure is established, showing users assigned to the nets, loading, and so on.

7. The Medical Scene Commander requests EMS dispatch to initiate a mass-casualty alert to all area hospitals. Hospitals page on-call emergency room staff in anticipation of the need to treat a significant number of casualties. The EMS dispatch requests additional ambulances from the Harvest Junction and Apple Valley ambulance companies, and paramedic supervisors are requested to respond. As ambulances are dispatched, their status is updated in the medical communications system. The Medical Scene Commander selects triage/treatment, transport, and logistics (equipment storage) areas, and identifies them on a map display; this location information is transmitted to the computing devices in other emergency medical vehicles. The Medical Scene Commander begins querying the medical communications system to identify the inventory of bed spaces at hospitals in the region, among other items. Hospital administrators begin evaluating patients to determine whether some can be released or moved to increase capacity for accommodating patients from the explosion.

8. As responders are dispatched or arrive on the scene, the medical communications system is updated. Their communications devices provide identifying information and geographic location. Identifying information includes name and agency as well as qualifications and skill sets. This data is available to the unified command, and to hospitals as required. Authentication of personnel from outside agencies is processed through a national database of qualified first responders.

5:25 PM

9. The EOD unit samples for any CBR release, and concludes that the device was a conventional explosive. Because of the initial explosion, the EOD unit is unable to conclusively check for a secondary explosive device using chemical sensors or canine units. The EOD personnel do not observe anything particularly unusual that would indicate a secondary device. The EOD unit commander communicates status to the Safety Officer, who informs the IC that responders may enter the inner perimeter. The IC broadcasts that responders can enter the inner perimeter, but to be on the lookout for anything that could indicate the presence of a secondary explosive device.

6. The topic of secondary explosive devices will be addressed in subsequent versions of the PS SoR. For more information, refer to the National Institute of Justice (NIJ) 2002 *Guide for Explosion and Bombing Scene Investigation.*

10. Fire units begin handling the burning cars as well as the lobby of the First National Bank building. The battalion chief quickly reviews the building plans and develops the approach for moving people out of the building, including those on upper floors. Firefighters also work their way to a stairwell where they can move to upper floors to aid in evacuation of the building. The firefighters deploy a series of short-range, high-bandwidth devices to extend the Incident Area Network (IAN) to transmit firefighter vital signs and video from helmet-mounted cameras back to the fire command.

11. EMS triage officers begin to attend to the victims in the area around the explosion, tagging people with transmitter tags. These tags have unique identifiers that include the color coding (red, yellow, green, black) and an embedded geolocation receiver. A time-stamped location of these victims is periodically transmitted to update the medical communications system language (while continuing to perform the primary communications functions of the PSCD).

12. EMS triage officers enter patient information (e.g., name and address) and condition into the medical communications system. The Medical Transportation Officer assigns patient transport based on status of hospital capacities, services available, and patient transports. As each assignment is made, the information is updated in the medical communications system.

13. A JIC is also established, and the Information Officer begins to coordinate with media representatives as they begin arriving on the scene.

5: 30 PM

14. Investigators arrive on the scene and begin interviewing witnesses. Investigators download stored video from the bank's surveillance cameras. The investigators rerun the video on a computer terminal and are able to reconstruct events occurring during the 30-minute period prior to the explosion. A late-model sports car is seen being parked next to the bank; it is apparently the source of the explosion. The investigators are able to identify the last three characters of the license plate. A wild-card query of that license plate with model information on the car is then run against local and state registration and stolen vehicle databases, and the National Crime Information Center (NCIC) stolen vehicle database. A matching vehicle is reported stolen in Metropolis in the northern part of the state.

    At this point the Federal Bureau of Investigation (FBI) Special Agent in Charge (SAC) for the Liberty County area is en route to the incident scene from his Central City office, along with other Federal agents in the area. The SAC is linked into the investigators' conversation. The investigators download the stolen automobile report from the Metropolis Police Department (MPD) and then contact the MPD investigator assigned to the case. The MPD investigator provides information on the primary suspect in the case, a student at the university identified by an eyewitness who placed the student with the stolen vehicle. A check by the FBI SAC confirms that this student is a known member of a foreign militant group; the SAC requests alerting the Central City and Metropolis Joint Terrorism Task Forces (JTTF).

5:35 PM

15. Command staff from CCPD begins initial staffing of the EOC, providing minimal coordination of resource management and interface to public and private organizations. The Central City DPW Street Maintenance Division is contacted to change traffic signals to steer traffic away from the area of the explosion and the key routes to the hospitals. Utilities are then contacted to shut off gas and electricity in affected area, and to monitor data for any signs of damage to subterranean utilities running beneath the scene of the explosion.

16. As ambulances begin removing injured victims from the area, police provide passage through the perimeter and provide traffic corridors to hospitals. The Transportation Officer notifies hospitals as ambulances depart for the hospitals; ambulance and patient status is updated in the medical communications system. At Central City Hospital, the ED doctor accesses the information in the medical communications system on a continuous basis until the particular patient arrives at the ER.

17. CSP units are assigned to secure other key sites in Central City and other cities in the state.

5:45 PM

18. LCSO deputies and CSP officers begin arriving on the scene. The CSP helicopter video system is linked to the Command Post and the EOC, and a general sweep of the area is initiated, allowing command staff to get an overall view of the incident scene. The video is also recorded for later use. The additional LE officers take over perimeter control, freeing up CCPD to control traffic along corridors to be used by ambulances transporting victims to hospitals, and to assist in the orderly evacuation of the other buildings on the street.

19. As more officers are assigned to perimeter control, the loading for that user group approaches 100 percent. The Communications Officer brings up a display of the user group assignments and informs the IC of the problem. The IC decides to break the perimeter control unit into two operating units, one for the east perimeter and one for the west perimeter. The change in operations is broadcast to the perimeter control user group. The Communications Officer splits the perimeter control user group into two separate user groups. The revised parameters of the PSCDs (such as operating frequencies) based on user group are automatically transmitted to the PSCDs assigned to that user group.

6:00 PM

20. CCPD officers assist in the evacuation of the buildings on either side of Y Street. Where feasible, they direct foot traffic to side and rear entrances to avoid crowding the area around the explosion scene. Officers identify persons with medical situations—a person apparently suffering a heart attack, 16 persons with non-life threatening cuts from flying glass. The CCPD officer notifies the police lead for evacuation, who requests assistance from the medical scene commander, who directs triage officers to provide assistance. The three-dimensional geolocation information of the police officer requesting assistance is displayed on the triage officer's computing device. The officer moves to the location, and moves patients to the triage/treatment area where EMS personnel attend to them.

21. EMS units are able to get to bodies that are trapped or near the previously burning vehicles. The triage officer tags nine victims as dead at the scene. Firefighters reach one badly injured victim who was apparently near the lobby windows when the explosion occurred. EMS personnel and firefighters enter the building and bring the victim back to the treatment/triage area.

6:15 PM

22. Firefighters report poor performance on their network to the Fire Battalion Chief at the unified command. The Fire Battalion Chief directs the Communications Officer to identify a solution. The Communications Officer assigns different frequencies for the net. The new performance parameters are then downloaded to the communications devices of all of the users on that temporary net.

23. The investigation continues. The MPD investigator identifies three people that she was preparing to interview as part of the stolen automobile investigation. The first is a professor at Metropolis

University; a conference call is set up involving the MPD and CCPD investigators, the FBI, and the professor. The professor states that the student has been in class during the time period up to and including the explosion. Investigators query all Arrest, Incident, and Citizen Stop reports from the databases of all agencies within the state for associates identified by the professor. The query identifies an associate as under investigation for being a member of a terrorist cell located in Metropolis.

24. The investigators access the JTTF database, obtaining a vehicle description and photograph of the second individual. This information is broadcast to all LE agencies in the region, and to handheld computing devices being carried by officers and agents working around the incident scene. An APB is issued to CCPD, LCSO deputies, surrounding county sheriff's departments, and the CSP. The CSP sets up roadblocks at locations around the perimeter of the city. The Transportation Security Administration (TSA) is notified at the airport, and the Coast Guard is notified to watch areas such as the marina at Bayport. FBI agents in Metropolis are also dispatched to the residences of the associate and other members of the cell.

6:40 PM

25. The last of the victims is transported to hospitals. Local ambulances are staged away from the scene, and other ambulances return to their home bases.

26. A CCPD officer patrolling the airport identifies the accomplice's vehicle parked in the parking garage and notifies the CCPD dispatch who notifies TSA. A user group is set up including CCPD and TSA officers. The airport management is notified, and the airport is closed down. LCSO deputies, CSP, and FBI agents arriving on the scene are added into the user group. After a 20-minute search, the suspect is located and immediately taken into custody.

7:00 PM

27. An electronic case file is begun collaboratively by the FBI, CCPD investigators, and MPD investigators, including an electronic request for warrants on the members of the terrorist cell under investigation; the warrant requests are sent to a judge who electronically signs them. FBI agents, working in conjunction with Metropolis PD officers, then execute the warrants.

28. Evacuation of the buildings is completed. CCPD officers involved in the evacuation are reassigned to inner perimeter control to protect the scene for evidence. LCSO deputies and CSP personnel are reassigned to the outer perimeter, and excess personnel are released.

7:15 PM

29. Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), local, and FBI evidence technicians begin to work at the site to collect evidence, reconstruct the blast, etc.

8:25 PM

30. The fire commander verifies that the fires in the First National Bank building are out. Firefighters remove the short-range network that was deployed in the building. All but one fire truck are released from the scene and return to firehouses.

9:00 PM

31. The final fire truck leaves scene, and the fire command post is removed. The LE command is moved into a vacant storefront office, and investigators begin the task of locating all bomb-related debris. The inner perimeter is expanded to include all of this debris. Bomb scene investigators

begin the arduous effort, which will consume most of the next 24 hours, of collecting, marking, and photographing all the evidence debris.

C.2.3 Transmission History

In the next table, *Security* indicates whether the transmission is secured (S) or unsecured (U).

Table 32: Transmission History Terrorist Car Bomb Scenario

Time: ID:	Response: PSAP, EOC, EMS, Fire, LE, Other:	Transmission Type and Net Utilization: Security:
Time: 17:00 ID: a1	PSAP: Receives numerous calls; geolocation information, including from cell phones, indicates area of impact	Transmission Type and Net Utilization: Voice Security: U
Time: 17:00 ID: a2	PSAP: Dispatches Fire Fire: Acknowledge	Transmission Type and Net Utilization: Voice or Binary Security: U
Time: 17:00 ID: a3	PSAP: Dispatches LE LE: Acknowledge	Transmission Type and Net Utilization: Voice or Binary Security: U
Time: 17:00 ID: a4	PSAP: Dispatches LE LE: Acknowledge	Transmission Type and Net Utilization: Voice or Binary Security: U
Time: 17:05 ID: b1	PSAP: Dispatches EOD team	Transmission Type and Net Utilization: Voice, Binary Security: U
Time: 17:05 ID: b2	LE: Police personnel from HQ arrive on scene; IC begins compiling roster of on-scene responders from geolocation information of responders	Transmission Type and Net Utilization: Binary Security: S
Time: 17:05 ID: b3	LE: LE officers arriving on the scene send authentication information and are registered in the on-scene responder database	Transmission Type and Net Utilization: Binary Security: S
Time: 17:05 ID: b4	LE: Officers assigned to perimeter control receive automated notifications	Transmission Type and Net Utilization: Binary Security: U
Time: 17:05 ID: b5	LE: User group established for outer perimeter control	Transmission Type and Net Utilization: Voice/High Security: U
Time: 17:05 ID: b6	LE: User group established for officers clearing area	Transmission Type and Net Utilization: Voice/High Security: U
Time: 17:05 ID: b7	EOC: User group established linking IC and EOC (command net)	Transmission Type and Net Utilization: Voice, Data/High Security: S

Table 32: Transmission History Terrorist Car Bomb Scenario (Continued)

Time: ID:	Response: PSAP, EOC, EMS, Fire, LE, Other:	Transmission Type and Net Utilization: Security:
Time: 17:05 ID: b8	PSAP: CCPD dispatch to LCSO and CSP dispatch for additional units LE: CCPD IC requests additional LE support	
Time: 17:10 ID: c1	Fire: Download building plans and site information	Transmission Type and Net Utilization: Binary, Images Security: U
Time: 17:10 ID: c2	PSAP: Video received from on-scene police car EOC: Video received from on-scene police car Fire: Video received by battalion chief being driven to scene LE: Police car arrives on scene and begins transmitting video from car-mounted camera	Transmission Type and Net Utilization: Video Security: U
Time: 17:20 ID: d1	LE: Communications Technical Officer accesses information from all responders' communications devices	Transmission Type and Net Utilization: Binary Security: S
Time: 17:20 ID: e1	PSAP: Issues Mass Casualty alert EMS: Requests dispatch issue Mass Casualty alert	Transmission Type and Net Utilization: Voice or Binary Security: U
Time: 17:20 ID: e2	Other: Hospitals page on-call staff	Transmission Type and Net Utilization: Binary Security: U
Time: 17:20 ID: e3	PSAP: Additional ambulances dispatched from other jurisdictions EMS: Acknowledge	Transmission Type and Net Utilization: Voice or Binary Security: U
Time: 17:20 ID: e4	EMS: Medical Scene Commander identifies triage, treatment, logistics, transport areas, map overlay sent to responding vehicles	Transmission Type and Net Utilization: Binary (Geospatial) Security: U
Time: 17:20 ID: e5	EMS: EMS responder status up-dated in medical communications system	Transmission Type and Net Utilization: Binary Security: U
Time: 17:20 ID: e6	EMS: User group established for responding EMS personnel	Transmission Type and Net Utilization: Voice Security: U
Time: 17:20 ID: e7	EMS: Medical Scene Commander queries medical communications system to inventory bed space, etc.	Transmission Type and Net Utilization: Binary Security: U
Time: 17:25 ID: f1	Fire: EOD notifies Safety Officer that area is clear	Transmission Type and Net Utilization: Voice Security: U
Time: 17:25 ID: f2	Fire: Commander broadcasts announcement that responders can enter inner perimeter	Transmission Type and Net Utilization: Voice Security: U
Time: 17:25 ID: g1	Fire: User group established for fire units on scene	Transmission Type and Net Utilization: Voice/Medium Security: U

Table 32: Transmission History Terrorist Car Bomb Scenario (Continued)

Time: ID:	Response: PSAP, EOC, EMS, Fire, LE, Other:	Transmission Type and Net Utilization: Security:
Time: 17:25 ID: g2	Fire: As fire units arrive on scene, authorization information is transmitted to update the roster of on-scene responders	Transmission Type and Net Utilization: Binary Security: S
Time: 17:25 ID: g3	Fire: Fire unit deploys net for video and "biometrics" from inside the building to fire command	Transmission Type and Net Utilization: Binary Security: S
Time: 17:25 ID: h1	EMS: EMS triage units begin tagging victims with RFID tags that transmit location and status information to Medical Scene Commander	Transmission Type and Net Utilization: Binary Security: S
Time: 17:25 ID: h2	EMS: Medical information entered into medical communications system for victims, including information on tags Other: As patients are assigned to different hospitals, medical staff at hospitals can download information as needed from medical communications system	Transmission Type and Net Utilization: Binary Security: S
Time: 17:25 ID: i1	LE: User group established for investigators	Transmission Type and Net Utilization: Voice, Binary, Image, Video/Medium Security: S
Time: 17:25 ID: i2	LE: Investigators download stored surveillance video from bank	Transmission Type and Net Utilization: Video Security: S
Time: 17:25 ID: i3	LE: Query on partial license number and car model information	Transmission Type and Net Utilization: Binary Security: S
Time: 17:25 ID: i4	LE: FBI added to investigators' net	Transmission Type and Net Utilization: Voice, Binary, Image, Video Security: S
Time: 17:25 ID: i5	LE: Download Incident Report on stolen car	Transmission Type and Net Utilization: Binary Security: S
Time: 17:25 ID: i6	LE: MPD investigator added to investigator's net	Transmission Type and Net Utilization: Voice, Binary, Image, Video Security: S
Time: 17:35 ID: j1	EOC: Contact utilities and Public Works	Transmission Type and Net Utilization: Voice Security: U
Time: 17:35 ID: k1	EMS: Central City Hospital ED access information in medical communications system, downloads patient vital information from en route ambulance	Transmission Type and Net Utilization: Binary Security: S
Time: 17:35 ID: l1	LE: CSP dispatched to protect other sites	Transmission Type and Net Utilization: Voice Security: U
Time: 17:45 ID: m1	LE: CSP helicopter downloads video to EOC, Unified Command	Transmission Type and Net Utilization: Video Security: S

Table 32: Transmission History Terrorist Car Bomb Scenario (Continued)

Time: ID:	Response: PSAP, EOC, EMS, Fire, LE, Other:	Transmission Type and Net Utilization: Security:
Time: 17:45 ID: m2	LE: CSP and Sheriff's deputies arriving on scene are added to various user groups	Transmission Type and Net Utilization: Voice Security: U
Time: 17:45 ID: m3	LE: User group established for officers working traffic detail for EMS ingress/egress	Transmission Type and Net Utilization: Voice/Medium Security: U
Time: 17:45 ID: m4	LE: IC notifies officers on perimeter control user group that net will be split	Transmission Type and Net Utilization: Voice Security: U
Time: 17:45 ID: m5	LE: Communications Officer downloads new parameters to split existing user group for perimeter control into two nets	Transmission Type and Net Utilization: Binary Security: S
Time: 17:45 ID: m6	LE: Automatic acknowledgement from radios receiving parameter changes sent to Communications Officer	Transmission Type and Net Utilization: Binary Security: S
Time: 18:00 ID: n1	LE: Police officers assist evacuation request medical assistance for victims	Transmission Type and Net Utilization: Voice Security: U
Time: 18:00 ID: n2	LE: Police team leader for evacuation requests assistance from Medical Scene Commander	Transmission Type and Net Utilization: Voice Security: U
Time: 18:00 ID: n3	EMS: Medical Scene Commander directs triage officers to assist police	Transmission Type and Net Utilization: Voice, Binary (Location Information) Security: U
Time: 18:05 ID: o1	Fire: Firefighters report communications problems on their user group	Transmission Type and Net Utilization: Voice Security: U
Time: 18:05 ID: o2	Fire: Communications Officer downloads new frequencies for PSCDs on user group	Transmission Type and Net Utilization: Binary Security: S
Time: 18:05 ID: o3	Fire: Automatic acknowledgement received from radios to confirm download	Transmission Type and Net Utilization: Binary Security: S
Time: 18:05 ID: o4	Fire: Firefighters confirm improved performance	Transmission Type and Net Utilization: Voice Security: U
Time: 18:15 ID: p1	LE: Professor on commercial phone service added to investigator net	Transmission Type and Net Utilization: Voice Security: S
Time: 18:15 ID: p2	LE: Investigators query records for all agencies in state	Transmission Type and Net Utilization: Binary Security: S
Time: 18:15 ID: p3	LE: JTTF members added to investigator's net	Transmission Type and Net Utilization: Voice, Binary, Image, Video Security: S

Table 32: Transmission History Terrorist Car Bomb Scenario (Continued)

Time: ID:	Response: PSAP, EOC, EMS, Fire, LE, Other:	Transmission Type and Net Utilization: Security:
Time: 18:15 ID: p4	LE: Investigators query JTTF database and obtain pictures of suspects	Transmission Type and Net Utilization: Binary, Image Security: S
Time: 18:15 ID: q1	LE: APB, including suspect's pictures, issued	Transmission Type and Net Utilization: Binary, Image Security: S
Time: 18:40 ID: r1	EMS: User group for EMS responders dissolved	
Time: 18:40 ID: s1	LE: CCPD officers identify suspect's car parked at airport	Transmission Type and Net Utilization: Voice Security: S
Time: 18:40 ID: s2	LE: Units assigned to airport, user group set up with CCPD, CSP, FBI, TSA agents	Transmission Type and Net Utilization: Voice Security: S
Time: 19:00 ID: t1	LE: Agents compile electronic case file and forward to judge	Transmission Type and Net Utilization: Voice, Binary, Image, Video Security: S
Time: 19:00 ID: t2	LE: Judge signs search warrants for execution	Transmission Type and Net Utilization: Binary Security: S
Time: 19:00 ID: u1	LE: LCSO and CSP personnel removed from net as they are released	
Time: 20:25 ID: w1	Fire: Short-range user group for fire units dissolved	
Time: 21:00 ID: x1	Fire: User group for fire units dissolved	

C.3 Scenario: Hurricane

This scenario is directly derived from the Hurricane Scenario in the July 2002 version of the National Incident Management System (NIMS). It was chosen so that personnel in interoperable communications can begin making their work more consistent with the current version of NIMS. Some information was eliminated to make the scenario briefer, and some added to make the communications aspects of the scenario the primary focus. Any deletions do not reflect a difference of opinion on any aspect of the original scenario.

C.3.1 Hurricane Scenario

1. The National Hurricane Center is forecasting a very active hurricane season, with the potential for the number of hurricanes to be significantly above normal. A few months following the hurricane prediction, the hurricane forecast center issues a warning that a rapidly developing storm could

directly impact the East Coast. The storm shows the indications that it could strengthen to a Category 5 hurricane.

2. Within days of the initial spawning of the hurricane, a slow-moving, Category 5 hurricane churns ashore, with its eye passing close to a large southern city. The forecast calls for a turn to the northeast where it could regain strength over open water, and make a second landfall further north, where the scenario takes place.

3. During the first landfall, the hurricane spawns heavy winds and rains, causing widespread wind and surge damage and flooding. Tens of thousands are forced to evacuate their homes, with damage to property and infrastructure forcing a delay in their return. Looting is reported to have occurred along empty coastal areas that were evacuated but not storm-ravaged. Flooding closes down several key highways, and access to and from the damaged area is problematic.

4. As the threat of an incident looming, the local, state, and regional EOCs in the scenario area rapidly gear up to prepare for and respond to incidents that the hurricane might spawn(e.g., pre-evacuate special needs populations, and direct citizens to begin boarding up windows). The planning and preparedness actions that have occurred in the Prevention Preparedness Council (PPC) prior to an incident transition into the execution of response plans within the EOCs.

5. Within 12 hours of landfall, a large fire starts in a warehouse district along the intercoastal waterway close to the ocean. The fire department responds establishing a unified command, with several engine companies being required to fight the fire as well as a fireboat company. The unified command works with the local EOC, which coordinates other hurricane preparation efforts. The local EOC coordinates with the state and regional EOCs to ensure the correct information is passed on the extent of the fires and that the unified command receives information about the hurricane. The unified command has access to browse extensive weather-related information via its command unit, as well as to receive special advisories and forecasting support from the EOC. The command unit is able to view the fire from several perspectives, including the fire trucks, several firefighters' helmets, the fireboat, and a dock camera. The EOC also has the ability to watch live video from the fire scene. Evacuations are ordered in anticipation of the hurricane, but some of the resources, including police units, normally used to assist in the evacuation are tied up in the fighting of the warehouse fire.

6. The oncoming hurricane requires tremendous interstate cooperation as large areas are ordered to be evacuated. The evacuations involve local and state LE, as well the highway department. The highway department is communicating hotspots directly to LE assigned to the evacuation, and LE is providing feedback and video back to the highway department so its personnel can make better routing decisions. The extensive evacuation is problematic because it ties up major routes and coordination with police, fire, and EMS units become strained. The ongoing fire has pulled significant police and fire resources away from the evacuation. The existing mutual aid resources are exceeded, requiring the local EOC to look to other inland jurisdictions for support. The local EOC begins coordination of resources and establishing public information announcements to ensure the public understands the gravity of the situation. The Public Information Officer (PIO) in the EOC is communicating directly to a fire department PIO in the unified command at the fire scene. The fireboat company, through discussions with the IC, the Coast Guard, and the EOC, has been released from the warehouse fire to batten down and prepare for the hurricane's landfall.

7. As the hurricane nears, and forecasts confirm a greater intensity and a landfall within 30 miles of the city, the local EOC recognizes the threatened level of potential damage will overwhelm mutual aid resources and capabilities. The EOC requests assistance from the state in evacuation and pre-staging response equipment. State police from outside jurisdictions are pulled in to help in the evacuation. Because of the challenges from traffic, the police use video, electronic maps, and other

real-time traffic data to navigate to the affected areas. As they arrive on scene, they are plugged into the existing command structure so that they can be effectively employed, and are provided with current weather and situational information. This also allows them to be accounted and planned for as the storm approaches.

8. A Category 5 hurricane potentially affecting several large metropolitan areas requires activation of, at a minimum, state EOCs in the affected areas, and leads to increased staffing at regional and national EOCs to support state and local planning and preparedness. The local EOCs work closely with the state EOCs to coordinate resources. The regional EOC reviews the situation to ensure proper Federal assistance is offered and provided in a timely manner.

9. The fire at the local warehouse district, despite the efforts of firefighters, rages out of control from high winds, and jumps to an adjacent warehouse complex. The IC has requested additional resources, and a separate IC has been set up to fight the second fire. The operations as well as the communications have been segmented into the two commands. An area command, run by the local fire department, is headed by the local Fire Chief, who is allocating now-scarce firefighting resources to both fires. The local EOC is coordinating the evacuation, made more difficult by the shutdown of a bridge within the vicinity of the warehouse fire and by the shortage of public resources to run the evacuation. The local EOC requests assistance from the state EOC for National Guard assistance to assist in the evacuation. The National Guard is able to come on site and communicate both with the EOC and existing local ICs.

10. The hurricane landfall is imminent amid the confusion of the ongoing warehouse fire. Using the real-time weather information and the advisories from the EOC, and with the safety of the firefighters in mind, the Fire Chief makes the decision to abandon the fire. The Chief orders the firefighters to move inland out of the danger of the predicted storm surge. Due to the rapid development of the storm, roads are still at a virtual standstill, with thousands of evacuees headed inland.

11. As the slow-moving hurricane approaches shore with 145 MPH winds, the initial devastation is immense. The eye remains a half-mile offshore as the storm parallels the coast. While the ensuing heavy rains douse the warehouse fire, the storm surge, winds, and rain combine to seriously affect the area's ability to respond effectively. The response community is essentially in a hunker-down mode as winds continue to batter the area.

12. After landfall of the hurricane, the local first responder resources become victimized themselves. Several fire stations suffer damage, as well as a large number of patrol cars. The communication infrastructure is significantly damaged. The cellular network is down, and the landlines have exceeded their capacity and have received some damage as well. With several towers damaged, individual communications devices must rely on the close proximity of a response vehicle, which acts as a high-power access point/repeater to the surviving tower infrastructure. As first responder resources arrive from outside of regional response areas, they must be able to integrate into the existing commands with their communication devices.

13. The storm was so strong during the extensive evacuation that drivers and their vehicles were caught trying to leave, and many deaths and injuries have been reported along the highways. Because of fallen trees, it could be days before some areas are reached. Many small communities have lost both landline communications and official radio communications because of extensive damage. Amateur radio operators are relaying some status information to the area EOCs. Hospitals are full. A Disaster Medical Assistance Team (DMAT[7]) and a Disaster Mortuary Operational

7. A Disaster Medical Assistance Team (DMAT) is a mobile medical field unit staffed and equipped to treat large numbers of injured.

Response Team (DMORT) will be arriving, and will need to communicate with the hospitals as they set up field sites. Search and rescue teams have been activated and also will be arriving. Amateur radio will provide the communication for many of these groups.

14. The forecast is for the storm to move further offshore, regain strength, and hit further north with the same relative intensity. The storm has rapidly taken on the gravity of a national incident, and it has only begun to make its ultimate effects known.

15. All affected state EOCs coordinate with regional EOCs in each potential major disaster area to work with local response organizations. At the regional level, they closely coordinate with each of the local Federal incident manager officials (FIMOs) to coordinate resources. An immediate need for National Guard resources is apparent at several locations, and several state governor offices and state EOCs have received requests to deploy those assets.

16. Reports begin to come in about looting in some counties that were evacuated but which lie slightly to the south, out of the main fury of the storm. National Guard assets have been requested to patrol those areas, but the requirement is outstripping available State Guard assets. As National Guard units arrive, they find it necessary to communicate with local responders more than usual because of the variety of support that they must provide due to the extensive area damage and disruption of first-responder infrastructure. The Bureau of Prisons has been asked to bring in some low-risk prisoners to aid in cleanup. The Bureau of Prisons must also integrate into the existing command and communication structure. The number of responders and the variety of response activities require existing systems to be flexible as incidents grow and shrink in number and extent and as massive resources are redeployed very frequently. There is a need to track these resources both within the incident and between incidents for responder safety and accountability.

17. Because of the extensive damage, outside resources will be deployed in the affected communities for an extended amount of time.

C.4 Scenario: Earthquake

C.4.1 Outline

1. Scenario Initiation: A 7.2-magnitude earthquake hits Central City.
2. The State Warning Center begins automated notifications.
3. The Public Safety Answering Point (PSAP) receives continuous calls.
4. PSAP dispatches first responders and alerts Emergency Management; helicopters are requested.
5. The EOC is activated.
6. Fire response and EMS arrive at scenes.
7. Radio Amateur Civil Emergency Service (RACES) begins providing communications support.
8. The Mayor notifies the Governor.
9. A unified command is formed onsite.

10. Urban search and rescue (US&R[8]) team and community emergency response teams (CERT[9]) are requested.
11. Central City requests county and state resources; the state mutual aid system is activated.
12. RACES assist outlying areas in the reporting of damages.
13. Staging areas are defined.
14. The Governor activates the National Guard and requests Federal assistance.
15. A conference call is held to identify additional resources requirements.
16. A JIC formed.
17. The state US&R arrives.
18. CERT Communication Team sets up.
19. The Red Cross establishes shelters, and public bus systems are commandeered for disaster support.
20. The DMAT team arrives; the coroner establishes a body collection and processing center.
21. The CERT Team provides information.
22. Structural specialists survey garage beneath damaged building.
23. Structural specialists warn of a potential building collapse.
24. Search team looks for victims.
25. A gas main has broken, the area is cordoned off.
26. Search teams enter the affected building; DMAT consults with other medical specialists.
27. The operational period ends; the IC rotates the team.
28. National Guard units begin arriving.
29. A Federal US&R team arrives.

C.4.2 Narrative

Santa Luisa County encompasses an area of about 2,800 square miles, bisected by the Santa Luisa Mountains. The county has a population of about 450,000. There are four incorporated cities (Central City, Fernwood, and Otsego on the southeast side of the mountains, and Cooney on the north side). There are two airports—Cooney Regional Airport (the former Cooney Air Force Base), and Santa Luisa Airport at Otsego. It is a summer weekday. At 9:00 a.m. the temperature at Santa Luisa airport was 80 degrees with a slight wind.

An earthquake of magnitude 7.2 hits the Central City area at 9:02 a.m., at the end of "rush hour." Damage to buildings and infrastructure is severe. Utilities are disrupted throughout the city and outlying area. The Cooney Canyon Nuclear Power Plant (CCNPP), located 11 miles outside of Cooney, suffers moderate damage, and requires an emergency shutdown of the plant and the declaration of a site area emergency. Damaged power lines ignite a number of brush fires in the mountains between the CCNPP and Central

8. An Urban Search and Rescue (US&R) team is a task force, complete with necessary tools and equipment, and required skills and techniques for the search, rescue, and medical care of victims of structural collapse.
9. Community Emergency Response Teams (CERT) are trained civilian volunteer auxiliary responders that assist victims and provide support for professional responders during a major disaster.

City. Ruptured natural gas lines lead to a number of residential structure fires. Ground-based, wire and fiber communications to the outside world are temporarily disrupted, and lines within the city, where operational, are immediately overloaded by calls from telephones that were knocked off the hook by the earthquake's shaking and by attempted calls by residents. Restoration of dial tone initially takes many minutes because of this overload. The 911 system remains fully operational due to the telephone company tandem switch into the PSAPs. However, many subscriber cables have been damaged, and the system as a whole suffers from the overload. The 911 system will be severely taxed for the first 12 hours, with only about 1 of 100 callers able to connect to the Central City PSAP.

The cellular system remains minimally operational, although the disruption to long-distance service generally prohibits calls outside of the city. The disruption to ground-based circuits leaves many tower sites isolated and out of service. Mobile-to-mobile calls within each cellular system function properly within areas served by operational towers, although circuits quickly overload from heavy traffic. Cellular 911 trunks linking the Mobile Switching Office to the PSAP remain operational. Thus cellular 911 calls are a significant source of information reaching the PSAP from public callers, particularly at the scenes of some of the major damage. As the incident proceeds, additional cell sites drop off the air as the site battery systems are depleted due to the loss of commercial power.

The county-wide microwave system, designed to withstand an event of this magnitude and linking all trunked public safety radio sites throughout Santa Luisa County, remains fully operational, including the dedicated private automatic branch exchange (PABX) switch that links all of the 911 PSAPs and public safety dispatch centers. The public safety radio system remains operational, as do communications with all mobile and portable subscriber units not damaged by the event. Additionally, at the county seat, the Santa Luisa County EOC has a ground station that is part of a statewide, satellite-based network operated by the Governor's Office of Emergency Management (OEM). This system provides a T-1 equivalent data circuit to Santa Luisa County that can be used for voice telephony, FAX, data, or video conferencing circuits. All are routed through a dedicated switch at the state EOC backed by a redundant switch at the alternate state EOC.

City, county, and state EOCs are equipped with integrated situational information systems designed to provide eagle-eye views of the overall incident as appropriate for that level of management, with the ability to drill down on any specific event or location to show details of the response to and management of it. This information can be shared in real time with field command posts, as well as with responding state and Federal resources. Through this integrated system, information can be retrieved from, and pushed to, the field units. This information system also gives resource managers the ability to monitor, query, and control resources at staging areas, as well as individual assets, in real time.

Note: ***Electronic communications among all of the personnel involved in this incident are authenticated. For local, on-duty personnel, this authentication takes place when each radio or computing terminal is initially logged on. For personnel responding from other local, state, and Federal jurisdictions, the authentication takes place at the time the unit initially joins the incident, and as different databases are queried or additional communications links established. A regional database processes the authentication of personnel from outside agencies.***

This scenario depicts the first 12 hours of Federal, state, county, and local public safety operations in response to this event.

9:02 AM

1. The local 911 PSAP immediately initiates internal operational and safety checks, noting it is operating on generator power with about 8 hours of fuel. As part of this effort, firefighters and building inspection personnel are dispatched to the PSAP. As the safety checks proceed, investigators use PSCDs to annotate areas of concern on building layout diagrams.

2. The nature of the event automatically activates the city EOC located in the police department immediately adjacent to, but separate from, the city PSAP in accordance with the city's All-Hazard Emergency Management Plan (EMP). The county EOC, located across the street from the city EOC, is automatically activated. The Regional Hospital Patient Management System is automatically activated, and communications links between hospitals are tested to ensure operability.

3. City and county public safety management personnel, many of whom were already at work, and other key city and county staff and volunteers who are assigned to the EOCs begin making their way to the centers. Staff includes members of the public works departments and local public utility representatives. They will track much of the disruption to gas, electricity, sewer, and water systems using a real-time geographic information system (GIS)-based system in the city and county EOCs. The nature of the event also causes automatic call-back of all off-duty city and county personnel. Call-back confirmations are made via voice radio or PSCDs as off-duty personnel begin responding. However, disruption to roads and the light rail system will delay many of these persons from reaching the EOCs for several hours.

4. In Capital City, an automated sensor system has detected the seismic event. The preliminary calculated magnitude of 7.0 causes a number of immediate and automated actions at the SWC operated by the OEM. Actions are based on a series of preprogrammed instructions for this type of event:

   - With a single “approval” entry to the OEM's CAD system, the state EOC is automatically activated, with computer-generated text paging alerts being transmitted across the state to state personnel via a number of commercial paging services. Automatic alerts are also sent to county and local officials and to staff and volunteers within a 100-mile radius of the calculated epicenter of the earthquake. The transmission of these notifications activates the state mutual aid system. Notification confirmations are made via telephone and PSCDs as personnel begin responding.
   - The SWC operator immediately contacts the control terminal for the National Warning System (NAWAS) headquartered at the FEMA operations center outside of Washington, DC. NAWAS is a wire-based, tie-line system linking all 50 states and major Federal Government facilities, including the Department of Defense. This alert is heard simultaneously by all of these facilities, many of whom initiate a preplanned call-up of personnel. Two centers monitoring this initial alert are the regional and national headquarters for FEMA. This alert begins a sequenced notification process to disaster personnel across the country who may be needed.
   - The SWC operator then notifies by telephone the Governor's staff, key legislators, and directors of all state public safety, resource and transportation agencies.

9:10 AM

5. The local 911 PSAP center responds to continuous emergency calls originating from cellular handsets and the few operating wireline telephones in the city. Observers state that a 10-story and a 14-story office building have collapsed, and a Federal building is near collapse. Many other buildings have sustained damage but appear to be structurally sound. Many people are reported

injured. The strong odor of natural gas in the downtown area, indicating the possibility of a gas explosion, is also reported. Reports of smoke in residential areas are received from citizens.

6. The PSAP dispatchers initiate first response to the various scenes by alerting the nearest available police, fire response, and EMS units. Fire units, following the CCFD's established seismic event response procedure, report the locations of structure fires on their PSCDs as they survey their initial response districts. The city's Mobile Command Center (MCC) is readied for deployment. The Emergency Manager also requests that state police helicopters be deployed to provide airborne video of the area; the helicopters are equipped with forward-looking infrared (FLIR) cameras enabling them to scan for hotspots indicating surface fires. The county PSAP, operated by the Santa Louisa Sheriff's Department (SLSD) dispatch, receives a call from the SWC via the satellite telephone requesting a preliminary damage assessment for forwarding to state and Federal agencies.

9:15 AM

7. The Emergency Manager, Mayor, and key city staff arrive at and activate the EOC to provide support to the IC and to coordinate the city's resources. Simultaneously, the county's Emergency Manager, County Executive, and key staff activate the county EOC to coordinate the response in the unincorporated areas to the CCNPP site area emergency, and to coordinate information flow and resource allocation to the incorporated jurisdictions within Santa Luisa County.

9:20 AM

8. Although hampered by disrupted roadways and debris, EMS, fire response, and police units respond to the various scenes. Injured persons who can be self-extricated, or easily extricated, are removed from the rubble and collected for transport to treatment centers. Assistance is offered to public safety personnel by many citizens who are now stranded at work sites. All patient names, medical conditions, receiving hospitals, etc. are entered into the EMS unit PSCDs to track the earthquake victims. Additionally, "captured public safety resources"—public safety personnel who work in other jurisdictions but cannot physically get there due to the damage—begin to check in at local fire houses and at the CCPD. Those who have their PSCDs with them are able to log into the local interoperability network and alert the EOC to their presence in Central City. The regional authentication database, housed at SLSD, provides authentication and privilege information as these personnel log in, and their location and personal information are added to the available personnel roster maintained by the logistics section at the city EOC. A similar process takes place within the county EOC for captured resources outside of the city, but within Santa Louisa County.

9. Pre-assigned members of the amateur radio community begin arriving at the EOCs and start staffing the amateur radio units located there. These RACES units provide logistical support to outlying agencies as well as communications support between an EOC and each of CCFD stations that have been designated as neighborhood emergency centers.

9:30 AM

10. Communications is established between the city and county EOCs, and with the SWC via the satellite system. The Governor, County Manager, Mayor and city and county emergency management directors are partied into a conference call via the very small aperture terminal (VSAT) system. Based on preliminary reports, the Governor directs his staff to begin preparing a disaster declaration. Critical response information is passed to responding mutual aid personnel as

they log into their local networks, and as they progress toward the scene through authenticated shared network access.

11. Field supervisors from CCPD begin arriving on scene at the major incidents, and assume the roles of local ICs. The assistant fire and police chiefs accompany the MCC to the field and assume overall IC responsibilities in a Unified Command structure, coordinating each of the individual sites. The ICs and communications unit leader, based on information being received from the field, set up the MCC in a location central to the major downtown high-rise collapses. In the MCC, the IC uses the PSCD to talk with the gas utility administrator and request the gas mains to city center be shut off. The IC requests that the DoT administrator as well as public works redirect traffic from the city center, and begin setting up an incident perimeter barrier that covers a 16-block area that allows only public safety traffic to enter. DoT uses ITS to reconfigure traffic signal lights, where connectivity and electrical power permit, and also to initiate warning messages to vehicle-mounted displays and VMSs along major roadways in surrounding areas in order to warn motorists to stay out of the incident zone. The IC makes additional resource requests to the EOC.

12. Two state police helicopters arrive in the area, and their video systems and FLIRs are linked to the MCC and the EOC. A general sweep of the area is initiated, allowing command staff to get an overall view; the video is recorded for later use.

13. The local jurisdiction's rescue and medical units are quickly being overwhelmed. The operations section chief requests assistance from several specialized US&R teams as well as CERTs.

14. Central City contacts the county EOC to request assistance from the county and state, including additional fire suppression resources, US&R task forces, and communications and logistics support. This request constitutes the formal activation of the state mutual aid system. One of the local US&R teams from the state Department of Forestry and Fire Protection (DFFP) is dispatched from Otsego and assigned to the search and rescue of victims in the two partially collapsed buildings. A DMAT from Capital City has been activated by the state, and a US&R Incident Support Team (IST)[10] is also deployed into the area. The state dispatches an OEM communications coordinator to the MCC to assess communications system integrity, and to coordinate DMAT and US&R communications resources. In anticipation of need, the OEM Communications Coordinator requests that a state OEM ICS type 1 communications unit and a trailer-mounted, high-capacity, satellite terminal be deployed to Central City.

15. Amateur radio operators communicating through the RACES communications unit at the county EOC have been reporting vegetation fires, damage to county roads and bridges, and rural residential damage in the county. The cities of Cooney, Fernwood, and Otsego report to the Santa Luisa County EOC via amateur radio and the county microwave voice and data network on conditions in their jurisdictions, and start requesting fire response, EMS, and public works resources.

10:45 AM

16. Based on three-dimension geolocation information coming from the field, the logistics section chief uses the PSCD's city map monitor to show the locations of the reported damage, and displays command post and other critical information for EMS, fire response, police, and public works staff in the operations section. This allows the most appropriate selection of staging areas. The information is simultaneously transmitted to displays in the MCC.

10. The Incident Support Team (IST) supports US&R teams with tasking, material, and coordination.

17. The Governor activates National Guard units. The Governor also requests that Federal assistance, including national US&R teams and a Mobile Emergency Response System (MERS) unit, be sent to Central City.

11:00 AM

18. Using their PSCDs and the satellite network, a conference call takes place between the logistics chiefs at the MCC, in the Central City EOC, Santa Luisa County EOC, state EOC, and the US&R IST, and with the on-scene OEM communications coordinator. Decisions are made to establish a resource mobilization center at the Santa Luisa County Fairgrounds, to colocate the IST at the mobilization center, and to establish a unified communications resource coordination point. The OEM communications coordinator is designated to serve as the area communications coordinator. Using the vehicle-mounted satellite terminal in the Center City MCC, the OEM communications coordinator contacts the state EOC with a request for a DFFP communications unit leader, and a communications coordinator from the National Incident Radio Support Cache (NIRSC) to assist with the unified resource coordination. The OEM coordinator then orders that the OEM transportable satellite unit and the type 1 communications unit be set up at the fairgrounds, and requests that two caches, or 56 units, of OEM-owned PSCDs be staged at the mobilization center for potential use. A request for fuel trucks to support city and county facilities, particularly the EOCs, is issued.

11:30 AM

19. As reporting teams from the local and regional media arrive on the scene, the Central City PIO forms a JIC in a building adjacent to the EOC, and uses PSCDs to produce maps directing the placement of camera teams away from areas requiring unrestricted emergency access. The JIC will also provide press releases with supporting video and still imagery that will be made directly available to media data feeds using the capabilities of responder PSCDs. The JIC will distribute information to the public regarding the location of food, potable water, shelter, and operational waste disposal facilities.

20. Upon arrival at the collapsed building, the DFFP US&R unit sets up a base of operations at a safe distance from the building, as directed by the staging manager. Using their PSCDs, the US&R personnel begin surveying for structural integrity and for likely victim locations. Their PSCDs set up an IAN that links with the MCC database and obtains blueprints and building drawings. The node allows various voice, video, and data to be transmitted to similarly equipped units, including the IST and the DMAT. It also provides three-dimensional location information for all PSCD-equipped personnel that are plotted into a GIS-based tracking system. As units survey the scene, they are able to overlay major structural displacements into the pre-event GIS database to allow improved structural analysis and determination of potential victim locations.

21. A CERT communication unit, an amateur radio operator, sets up in close proximity to the MCC and, working through the liaison officer, verifies a process to pass intelligence and logistics information from CERT to the US&R branch.

22. The Red Cross has set up a command post next to the MCC, and has activated shelters in several local schools. Red Cross personnel are capturing on their PSCDs the names of every person arriving at the shelters, and relaying the information to a central database that other parties can access. This information is available to the Red Cross representative in the EOC, as well as to key city officials. City public buses and public school buses, both of which operate on the public safety radio system, are alerted and organized to support transport of victims and the public to treatment facilities or shelters.

2:00 PM

23. The DMAT from Capital City has arrived and is setting up its unit. All patient names, medical conditions, etc. will be entered into PSCDs to track the earthquake victims. The SLSD coroner's unit begins setting up a central DMORT center for processing the dead, including collection of names and identifying information, as well as for the long-term storage of bodies. As bodies are brought to the collection point, critical data, including the location where they were found, are stored in a special central database.

24. CERT teams are becoming more organized as they search though residential areas for trapped victims. As they come across larger or more questionable structures, they request assistance from a US&R team as well as provide damage information through the CERT communications unit. PSCDs are linked to the city GIS system to log activities of these teams.

4:00 PM

25. Structural specialists begin the structural survey of the parking garage, using handheld PSCDs to sketch the structure perimeter, noting entrances and areas of structural concern. The survey data is wirelessly sent to the US&R's node where it is coordinated with pre-event GIS information. At the same time, a group of structural engineers begin looking over the drawing and blueprints for the buildings. Data collected indicates that a larger building is on the verge of collapse within the next 24 hours. This information is relayed to all public safety units via the PSCDs, and to the command post established at the park. This information is then transmitted to the IC, who can make entry plans from this data. Using this data, IC establishes the hazard zone for tracking entry into the garage and the collapsing building. At the same time, the data is relayed from the MCC through the satellite network to the IST at the mobilization center to assist in its long-range planning.

26. The structural specialists find that one outside wall of the parking garage has fallen away and the concrete T-bars of the parking garage have detached from the outside wall, collapsing it. The engineering team at the Federal building finds that a gas main on the north side of the building was ruptured, with leaking and trapped gas posing an explosion hazard. The gas utility representative in the EOC is requested to ensure that gas mains are off and, where the gas valve control system may have failed, that dispatch personnel manually check and secure valves. The police are directed to cordon off a four-square-block area and begin necessary evacuations. The structural specialists set up two theodolites[11] to monitor any movement of the Federal building. These units contain video cameras that transmit images via an integrated broadband transmitter to the base of operations, where the specialists can safely monitor the structure. Once a preliminary structural assessment is complete, the IC assigns the search teams to enter the structure to search for victims. The teams are assisted by hazardous materials (Hazmat) specialists, who detect any nuclear, biological, or chemical hazards to the rescue personnel. A search of the appropriate databases allows for an inventory of the building contents to be reviewed, examined, and the results transmitted to all officials involved.

27. Two search teams that will enter the garage area and Federal building turn on their personal safety systems, which include activity monitor and three-dimensional location tracking systems. As the teams enter the hazard zone, they check in with a safety officer, who notes their entry using a PSCD. This information is used at the base of operations to track all personnel inside the hazard zone. As the search teams search, they note the presence or absence of victims on their PSCDs, and the data is displayed on the floor plan of the structure at the base of operations. As the teams

11. A theodolite is a surveying instrument that can be used to measure and monitor movement of an object.

move through the garage, the locations of all team members are logged for use if a member becomes lost or incapacitated.

28. The Hazmat Team links its hand-held monitoring equipment into a PSCD, which relays any detection information to a safety officer's terminal at the MCC. As search team 2 proceeds into the parking garage, the Hazmat team detects a potentially dangerous level of gasoline vapor in the air. A safety officer's instrument indicates the danger, and he decides that this route into the garage is too hazardous. He orders the team out of the garage, and to find another entrance. Before the team exits, they leave a remote combustible gas detector. This terminal will continuously monitor the air and, if an explosive condition is detected, will send an evacuation signal to all personnel in the structure.

29. Search team 2 uses their voice radios and PSCDs to coordinate their search, and the search team leader uses his PSCD to report the team's progress to the IC. Team 2 locates several victims trapped in vehicles under the concrete T-bar sections, and notes their locations on the PSCDs. The IC calls for a rescue team to go to the garage to assist in the rescue operation. Rescue team 1 begins work on the extrication of the victims. As the rescue team accesses each patient, medical specialists treat the patient as much as possible in the confined space.

30. The medical team managers use their PSCDs at the base of operations to inform the IST and the DMAT of the number of victims, the severity of their injuries, and the estimated time of their extrication. When it is decided that one of the victims requires a leg amputation before extrication, the medical specialists consult with the medical team managers using voice and video exchange with their PSCDs.

31. Due to the number of victims in the immediate area, the demand for communications exceeds the available capabilities. The PSCDs execute prioritization routines that prioritize communications based on need. Voice communications are given top priority, vital medical data is given second priority, medical video data is scaled back to fewer frames per second, and on-scene medical personnel prioritize individual cases so that video is periodically dropped for lower-priority patients.

6:00 PM

32. The IC, safety officer, and operation section chief use data on the total time each team has been in the structure to rotate teams for rest and rehabilitation. Eventually, all victims in the garage are extricated, stabilized, and transported to the DMAT. The IC then contacts the logistics section chief for re-supply of expended equipment and material, and discusses priorities and the team's next assignments with the planning section chief.

33. National Guard units activated by the Governor begin arriving. These units are seamlessly integrated into the communications network using their own PSCDs.

9:00 PM

34. A Federal US&R task force, flown by military air transport to Cooney Regional Airport, arrives to support the ongoing effort. Its voice and data PSCDs are entered into the regional authentication database and the communications unit leader authorizes their participation. They join the incident's network. The task force's leader uses his PWD to send the personnel and equipment manifests to the IST at the mobilization center. The task force uses robotic units capable of remotely providing video, audio, and sensing information from inside the building. The units transmit their information to the US&R incident base.

C.4.3 Transmission History

Though not reiterated in the following table, note that the transmission IDs a2 and a3 are repeated numerous times during the course of the scenario as teams check the structural integrity of key facilities in the area.

Table 33: Transmission Record Earthquake Scenario

Time: ID:	Response: PSAP, EOC, Police, Fire, EMS, Other:	Transmission Type:
Time: 9:02 ID: a1	PSAP: Fire and building inspectors dispatched to PSAP Fire: Dispatched to PSAP Other: Building inspectors dispatched to PSAP	Transmission Type: Binary (Fire), Voice (Inspectors)
Time: 9:02 ID: a2	Other: Building inspectors download building plans	Transmission Type: Binary
Time: 9:02 ID: a3	Fire: IAN established for firefighters and building inspectors at PSAP building Other: IAN established for firefighters and building inspectors at PSAP building	Transmission Type: Voice, Binary
Time: 9:02 ID: a4	EOC: City/county EOC activated and key staff alerted	Transmission Type: Binary, Text
Time: 9:02 ID: a5	EOC: Incident area network established for key staff (emergency manager, mayor, county exec, etc.) en route to Operations Center	Transmission Type: Voice
Time: 9:02 ID: a6	EOC: Callback of off-duty workers	Transmission Type: Binary
Time: 9:02 ID: b1	EOC: State EOC activated; SWC automatically notifies state personnel	Transmission Type: Text
Time: 9:02 ID: b2	EOC: SWC notifies surrounding counties	Transmission Type: Text
Time: 9:02 ID: b3	EOC: SWC notifies NAWAS	Transmission Type: Binary via Wire-Based Tie Line
Time: 9:02 ID: b4	EOC: FEMA regional and national Operations Centers begin alerting of disaster personnel across the country	Transmission Type: Binary via Wire-Based Tie Line
Time: 9:02 ID: b5	EOC: SWC operator notifies governor's staff, key legislators, state agency heads	Transmission Type: Voice via Telephone
Time: 9:10 ID: c1	PSAP: Continuous incoming calls	

Table 33: Transmission Record Earthquake Scenario (Continued)

Time: ID:	Response: PSAP, EOC, Police, Fire, EMS, Other:	Transmission Type:
Time: 9:10 ID: d1	PSAP: Dispatch police, fire, and EMS Police: Units dispatched to area Fire: Units dispatched to area EMS: Units dispatched to area	Transmission Type: Binary
Time: 9:10 ID: d2	Fire: Fire units report locations of structure fires	Transmission Type: Binary
Time: 9:10 ID: d3	PSAP: Receives request for preliminary damage assessment EOC: SWC sends request for preliminary damage assessment	Transmission Type: Binary via VSAT
Time: 9:15 ID: e1	EOC: Emergency managers and key city and county staff arrive; as they arrive on scene they are removed from temporary net	
Time: 9:20 ID: f1	Police: Police, fire response, and EMS begin arriving at various scenes; at each scene an IAN is established for all first responders on scene	Transmission Type: Voice
Time: 9:20 ID: f2	EMS: EMS units begin transporting victims to hospitals; patient vital signs relayed to hospitals; status information relayed to EOC	Transmission Type: Voice, Binary
Time: 9:20 ID: g1	Other: RACES sets up at EOC, fire stations, and outlying agencies	Transmission Type: Voice, Binary
Time: 9:20 ID: h1	EOC: User group established between city/county EOC, SWC, and Governor's office	Transmission Type: Voice via VSAT
Time: 9:30 ID: i1	Police: Field supervisors beginning to arrive at scenes, establish IC Fire: MCC deployed at scene of building collapse; user group established linking site commanders, MCC, and EOC	Transmission Type: Voice
Time: 9:30 ID: i2	Police: User group established linking on-scene commanders to EOC Fire: User group established linking on-scene commanders to EOC	Transmission Type: Voice
Time: 9:30 ID: i3	Police: As first responders arrive at each scene, register electronically to be added to on-scene roster and included in incident area network	Transmission Type: Binary
Time: 9:30 ID: i4	Police: State police helicopters sent to area to perform aerial reconnaissance; video linked to EOC and MCC; pilots added to temporary net for command	Transmission Type: Video, Voice

Table 33: Transmission Record Earthquake Scenario (Continued)

Time: ID:	Response: PSAP, EOC, Police, Fire, EMS, Other:	Transmission Type:
Time: 9:30 ID: i5	Fire: Overall IC contacts gas utility to shut off gas mains to city center	Transmission Type: Voice
Time: 9:30 ID: i6	Fire: IC contacts city DPW to redirect traffic and establish barricades	Transmission Type: Voice
Time: 9:30 ID: j1	Fire: Operations Section Chief requests US&R and CERT	Transmission Type: Voice
Time: 9:30 ID: k1	EOC: Mayor requests state US&R and DMAT teams	Transmission Type: Voice via Telephone
Time: 9:30 ID: k2	EOC: State dispatches OEM Communications capability to Central City with reach back capability to state OEM	Transmission Type: Voice, Binary, Image, Video via Infrastructure, VSAT
Time: 9:30 ID: l1	Other: RACES operators report damage outside Central City and relay requests for assistance form outlying cities	Transmission Type: Voice, Binary
Time: 10:45 ID: m1	EOC: Display shows location of units (from reported three-dimensional geolocation), damage reports on map; information used to select staging areas Fire: Display shows location of units (from reported three-dimensional geolocation), damage reports on map	Transmission Type: Binary (Three-Dimensional Geolocation)
Time: 11:00 ID: n1	EOC: Governor activates National Guard, requests national US&R and MERS assistance	
Time: 11:00 ID: o1	EOC: Conference call	Transmission Type: Voice via VSAT
Time: 11:30 ID: p1	Fire: PIO uses location and damage information for placement of media teams, generates video and images that are transmitted electronically to media representatives	Transmission Type: Binary, Image, Video
Time: 11:30 ID: q1	Other: DFFP US&R arrives, added to IAN; tactical user group also established	
Time: 11:30 ID: q2	Other: Short-range broadband net established to relay video, marked-up blueprints, and images among IC members	
Time: 11:30 ID: r1	Fire: CERT communication team sets up link to US&R	Transmission Type: Binary, Image, Video
Time: 11:30 ID: s1	Other: Red Cross sets up emergency shelters; user group to link Red Cross representatives with EOC; link used to exchange data on survivors, status	Transmission Type: Voice, Binary

Table 33: Transmission Record Earthquake Scenario (Continued)

Time: ID:	Response: PSAP, EOC, Police, Fire, EMS, Other:	Transmission Type:
Time: 14:00 ID: t1	EMS: DMAT deploys; links to EOC Medical Coordinator and hospitals to exchange victim data; DMAT commander added to command network	Transmission Type: Voice, Binary
Time: 14:00 ID: u1	Other: CERT team commanders are linked in a user group with EOC; when necessary linked into US&R temporary net as well	
Time: 16:00 ID: v1	Other: Structural specialists are linked into US&R IAN	Transmission Type: Voice, Binary
Time: 16:00 ID: v2	EOC: Structural data is overlaid with blueprint information	
Time: 16:00 ID: v3	EOC: Structure risk broadcast to all units	Transmission Type: Voice, Binary
Time: 16:00 ID: v4	Fire: IC establishes hazard zone, requests barricades from Central City DPW streets maintenance to establish perimeter	Transmission Type: Voice
Time: 16:00 ID: w1	Other: team informs IC of ruptured gas line	Transmission Type: Voice
Time: 16:00 ID: w2	Fire: IC directs police to establish perimeter area around gas	Transmission Type: Voice
Time: 16:00 ID: w3	Other: Structural specialists set up theodolites	Transmission Type: Binary, Video
Time: 16:00 ID: w4	Fire: Hazmat team queries database to identify any potential hazards in building	Transmission Type: Binary
Time: 16:00 ID: w5	Other: Structural specialists verify structural integrity	Transmission Type: Voice
Time: 16:00 ID: w6	Fire: IC directs search and Hazmat teams to enter building to search for victims; incident area network for personnel in building established	Transmission Type: Voice
Time: 16:00 ID: x1	Other: Search teams entering garage area establish IAN for activity monitoring and location information; data (such as location and status of victims) is also transmitted	Transmission Type: Binary
Time: 16:00 ID: y1	Fire: Hazmat team links monitoring equipment to communications network; information transmitted to on-scene commander and MCC	Transmission Type: Binary
Time: 16:00 ID: y2	Fire: Units ordered out from structure	Transmission Type: Voice

Table 33: Transmission Record Earthquake Scenario (Continued)

Time: ID:	Response: PSAP, EOC, Police, Fire, EMS, Other:	Transmission Type:
Time: 16:00 ID: y3	Fire: Units leave behind remote monitor	Transmission Type: Binary
Time: 16:00 ID: z1	Other: Search teams continue searching garage	Transmission Type: Voice, binary
Time: 16:00 ID: z2	EMS: Rescue team attends to victims; medical status and video transmitted to hospitals; due to data exceeding available bandwidth, degraded bandwidth management is in effect	Transmission Type: Voice, Binary, Video
Time: 18:00 ID: aa1	EOC: IC staff uses activity data to rest and rotate search and rescue teams	Transmission Type: Voice, Binary
Time: 18:00 ID: bb1	Other: National Guard begins arriving; command added to command network; officers added to IAN at specific scenes where they are working with first responders	Transmission Type: Voice, Binary
Time: 21:00 ID: cc1	Other: Federal US&R team arrives; command network added; unit personnel added to on-scene responder rosters; robotic unit deployed with short-range communication for transmitting video from inside collapsed buildings; video transmitted when requested to MCC and EOC	Transmission Type: Voice, Binary, Video

This page intentionally left blank.

Appendix D References

D.1 Print References

(Irving, 1996)	Irving, Larry, *Final Report of the Public Safety Wireless Advisory Committee (PSWAC) to the Federal Communications Commission and the National Telecommunications and Information Administration*, September 11, 1996.
(PS SoR Volume II, version 1.0, 2006)	*Public Safety Statement of Requirements for Communications & Interoperability, Volume II: Quantitative*, Version 1.0, October 2006.

D.2 Online References

National Institute of Justice (NIJ), *A Guide for Explosion and Bombing Scene Investigation*, 2000. http://www.bombsecurity.com/downloads2/nij_181869.pdf. Cited August 2006.

National Highway Traffic Safety Administration, Emergency Medical Services Agenda for the Future, 1996. http://www.nhtsa.dot.gov/people/injury/ems/agenda/emsman.html. Cited August 2006.

National Incident Management System (NIMS), *NIMS Basic: The Incident Command System*, FEMA 501-8, March 27, 2006, Revision 0. http://www.fema.gov/pdf/nims/NIMS_basic_incident_command_system.pdf. Cited August 2006.

Federal Communications Commission (FCC) OET Bulletin No. 65 (August 1997): *Evaluating Compliance With FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields*. http://www.fcc.gov/oet/rfsafety/. Cited August 2006.

This page intentionally left blank.