PUBLIC SAFETY

CHAPTER 16

SAFETY AND SECURITY ARE VITAL TO AMERICA'S PROSPERITY. Broadband can help public safety personnel prevent emergencies and respond swiftly when they occur. Broadband can also provide the public with new ways of calling for help and receiving emergency information.

A cutting-edge public safety communications system uses broadband technologies:

- To allow first responders anywhere in the nation to send and receive critical voice, video and data to save lives, reduce injuries and prevent acts of crime and terror.
- To ensure all Americans can access emergency services quickly and send and receive vital information, regardless of how it is transmitted.
- To revolutionize the way Americans are notified about emergencies and disasters so they receive information vital to their safety.
- To reduce threats to e-commerce and other Internet-based applications by ensuring the security of the nation's broadband networks.

Unfortunately, the United States has not yet realized the potential of broadband to enhance public safety. Today, first responders from different jurisdictions and agencies often cannot communicate during emergencies. Emergency 911 systems still operate on circuit-switched networks. Similarly, federal, Tribal, state and local governments use outdated alerting systems to inform the public during emergencies.

The United States also faces threats to the resiliency and cybersecurity of its networks. As the world moves online, America's digital borders are not nearly as secure as its physical borders.

The country must do better. In a broadband world, there is a unique opportunity to achieve a comprehensive vision for enhancing the safety and security of the American people. Careful planning and strong commitment could create a cutting-edge public safety communications system to allow first responders anywhere in the nation to communicate with each other, sending and receiving critical voice, video and data to save lives, reduce injuries and prevent acts of crime and terror.

Broadband can also make 911 and emergency alert systems more capable, allowing for better protection of lives and property. For example, with broadband, 911 call centers (also known as public safety answering points or PSAPs) could receive text, pictures and videos from the public and relay them to first responders. Similarly, the government could use broadband networks to disseminate vital information to the public during emergencies in multiple formats and languages.

Finally, well-structured and well-protected broadband networks could reduce threats to Internet-based applications. The proliferation of Internet Protocol (IP)-based communications requires stronger cybersecurity. Disasters and pandemics can lead to sudden disruptions of normal IP traffic flows. As a result, broadband communications networks must be held to high standards of reliability, resiliency and security.

The recommendations in this chapter are designed to realize this vision.

RECOMMENDATIONS

Promote public safety wireless broadband communications

- Create a nationwide interoperable public safety wireless broadband communications network (public safety broadband network).
- Survey public safety broadband wireless infrastructure and devices.
- Ensure that broadband satellite service is a part of any emergency preparedness program.
- Preserve broadband communications during emergencies.

Promote cybersecurity and the protection of critical broadband infrastructure

- The Federal Communications Commission (FCC) should issue a cybersecurity roadmap.
- The FCC should expand its outage reporting requirements to broadband service providers.
- The FCC should create a voluntary cybersecurity certification regime.
- The FCC and the Department of Homeland Security (DHS) should create a cybersecurity information reporting system (CIRS).
- The FCC should expand its international participation and outreach.
- The FCC should explore network resilience and preparedness.
- The FCC and the National Communications System (NCS) should create priority network access and routing for broadband communications.
- The FCC should explore broadband communications' reliability and resiliency.

Encourage innovation in the development and deployment of Next Generation 911 (NG 911) networks and emergency alert systems

- The National Highway Traffic Safety Administration (NHTSA) should prepare a report to identify the costs of deploying a nationwide NG 911 system and recommend that Congress consider providing public funding.
- Congress should consider enacting a federal regulatory framework.
- The FCC should address IP-based communications devices, applications and services.
- The FCC should launch comprehensive next-generation alert system inquiry.
- The Executive Branch should clarify agency roles on the implementation and maintenance of a next-generation alert and warning system.

16.1 PROMOTING PUBLIC SAFETY WIRELESS BROADBAND COMMUNICATIONS

RECOMMENDATION 16.1: Create a public safety broadband network.

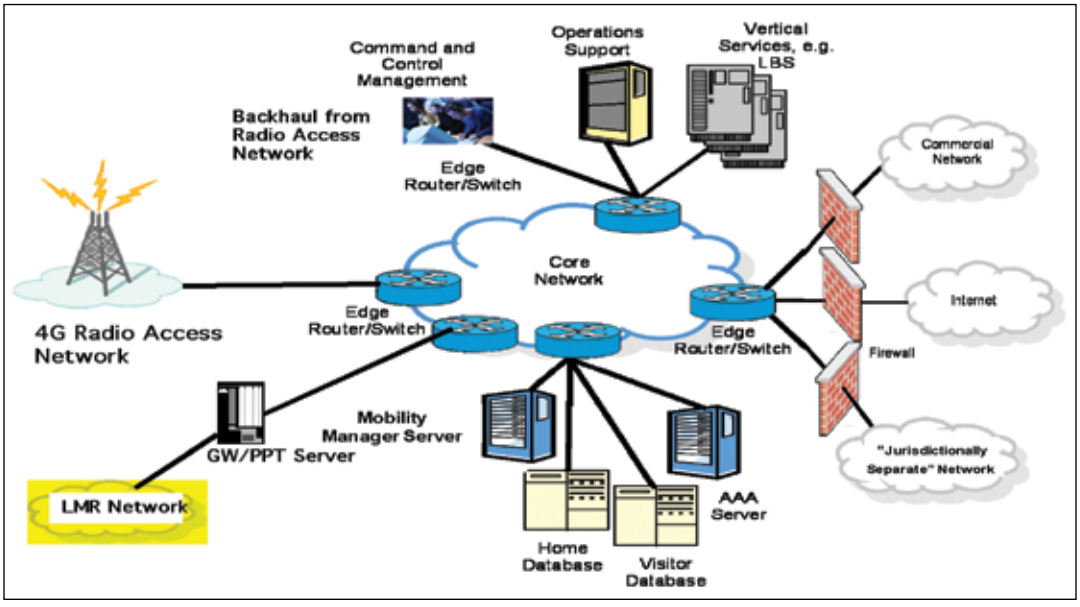
- **Create an administrative system that ensures access to sufficient capacity on a day-to-day and emergency basis.**
- **Ensure there is a mechanism in place to promote interoperability and operability of the network.**
- **Establish a funding mechanism to ensure the network is deployed throughout the United States and has necessary coverage, resiliency and redundancy.**
- **Conform existing programs to operate with the public safety broadband network.**

The country has long recognized the potential for broadband technologies to revolutionize emergency response wireless mobile communications. This technology will give first responders new tools to save American lives. The country needs a public safety broadband network that allows first responders to communicate with one another. A three-pronged approach will allow the speedy deployment, operation and continued evolution of such a network.

First, an administrative system must ensure that users of the public safety broadband spectrum have the capacity and service they require for their network and can leverage commercial technologies to capture economies of scale and scope. There are significant benefits, including cost efficiencies and improved technological advancement, if the public safety community can increasingly use applications and devices developed for commercial wireless broadband networks. Ultimately, this system must be flexible, allowing public safety entities to forge incentive-based partnerships with commercial operators and others.[1]

This system will allow the public safety community to realize the benefits of commercial technologies, which will reduce costs and ensure the network evolves. However, leveraging

Exhibit 16-A: Public Safety Broadband Network Architecture[3]



commercial broadband will not be sufficient to develop a truly interoperable nationwide network that meets public safety standards. To ensure the necessary resiliency, capacity and redundancy, the public safety community should be able to roam and obtain priority access on other commercial broadband networks. Commercial operators will need to be compensated at a reasonable rate for this service.

Past efforts to create a public safety narrowband interoperable voice network have failed. Data suggest that many public safety radio systems lack basic interoperability. They also suggest that most jurisdictions that have improved their systems still only have an "intermediate" level of interoperability at best—not the advanced level of interoperability that is required for truly seamless communications in the event of a major emergency.[2] The public safety broadband network offers a new opportunity to achieve advanced interoperability now.

In addition to a strong administrative system, the FCC should also create an Emergency Response Interoperability Center (ERIC) to ensure that these applications, devices and networks all work together, so that first responders nationwide can communicate with one another seamlessly. In addition, the Federal Emergency Management Agency (FEMA) should undertake a survey to track progress on broadband interoperability for the public safety community. ERIC will set the course for interoperability immediately and ensure it is maintained. Focusing on interoperability from the beginning should help the public safety broadband network to overcome the difficulties faced by other earlier voice efforts.

Finally, a grant program will be designed to provide federal support to local efforts in order to fund the capital and ongoing costs of the public safety broadband network. The grant program must provide public safety network operators with long-term support and enough flexibility to form appropriate partnerships with systems integrators and other vendors to ensure the public safety broadband network is deployed properly.

BOX 16-1:

Realizing the Promise of Broadband to Improve Emergency Medical Response

Cardiologist Richard Katz knows the life-saving potential of broadband. During an FCC field hearing at Georgetown University Medical Center, the George Washington University (GWU) professor of medicine vividly detailed how wireless broadband technologies can help him provide emergency medical care. A "smart band-aid" attached to an accident victim's chest or wrist can detect vital signs and wirelessly transmit this information to Dr. Katz over GWU's mVisum network. He can receive electrocardiograms of "pristine" quality on his cell phone. And he can use his phone to access patient medical records and disseminate emergency messages and alerts. In short, broadband technologies allow Dr. Katz to integrate aspects of medical care, improving his ability to offer assistance during a disaster or other emergency.

Administrative System

In 1997, Congress directed the FCC to provide public safety agencies with spectrum in the 700 MHz band, considered prime spectrum for public safety communication. In 2007, the FCC adopted rules to promote the construction, deployment and operation of a nationwide and seamless wireless 700 MHz public safety broadband network[4] by creating a mandatory partnership between the public safety community and the private licensee of a 700 MHz commercial spectrum allocation known as the "D block." The FCC subsequently held an auction in which the D block spectrum failed to attract a required minimum bid. There are many possible reasons for this failure.[5]

The FCC should overcome past challenges by encouraging, though not requiring, incentive-based partnerships to ensure success. The FCC should encourage network solutions that reduce costs and should provide options for the public safety community to leverage commercial networks, private networks or both.[6] These rules should also provide the public safety community with more competitive choice among commercial partners. In addition, once the new network is able to support "mission critical" voice communications, the FCC should evaluate the spectrum requirements necessary to ensure adequate capacity for that use, as well as for existing networks. Ultimately, a more flexible set of rules should allow a better balance between the needs of the public safety community and the companies that will partner to build this network.

In more detail, this administrative system should include:

- *An opportunity to enter flexible spectrum-sharing partnerships with commercial operators.* The public safety community must be able to partner with commercial operators and others (such as systems integrators) to lower the costs of building the network and encourage its evolution. Unlike the previous approach that focused solely on the D block, an incentive-based partnership model that addresses not just the D block, but commercial wireless spectrum more broadly, will provide enhanced flexibility and the benefits of economies of scale. Such partnerships should be subject to interoperability requirements set forth by ERIC. Public safety licensees should also be able to allow non-public safety partners to use their spectrum on a secondary basis—that can be preempted—through leasing or similar mechanisms. Partners could include critical infrastructure users such as utilities connecting to the Smart Grid.[7] However, any revenues

received by a public safety entity for such use must be used to build or improve the public safety broadband network.

- *Public safety access to roaming and priority access on commercial networks.* To improve the capacity of public safety networks during emergencies, the FCC should begin a rulemaking to require commercial mobile radio service providers to give public safety users the ability to roam on commercial networks in 700 MHz and potentially other bands. The public safety community should have this ability both in areas where public safety broadband wireless networks are unavailable and where there is currently an operating public safety network but more capacity is required to respond effectively to an emergency.

  The rulemaking also should stipulate that, when a public safety broadband wireless network is at capacity or unavailable, authorized public safety users should get priority access on commercial networks, including all networks using the 700 MHz band and potentially other networks as well. The licensee(s) should be able to obtain priority access under terms similar to those required in today's Wireless Priority Service (WPS). But, unlike WPS, this capacity should be available for state and local first responders as well as National Security/Emergency Preparedness (NS/EP) communications. In addition, the priority access framework should take advantage of the additional access and prioritization capabilities of 4G wireless technologies. Unlike today's circuit-switched cellular networks, 4G wireless networks can give public safety data immediate priority without waiting for commercial capacity to be freed up. Commercial operators should receive reasonable compensation for public safety priority access and roaming capabilities on their networks.
- *Licensing the D block for commercial use, with options for public safety partnership.* The FCC should quickly license the D block for commercial use, while implementing several requirements for the D block licensee(s) to maximize options for partnerships with public safety. First, the FCC should require the D block licensee(s) and the public safety broadband licensee(s) each to operate their networks using the same air interface technology standard. The emerging consensus of the public safety community and carriers is that 700 MHz networks will use the Long Term Evolution (LTE) family of standards. The FCC should consider designating this standard.[8] A consistent air interface creates a greater likelihood of interoperability between the public safety and commercial D block networks. It will facilitate roaming between networks to improve coverage and access for public safety and commercial customers. In addition, a consistent air interface will encourage a larger number of potential users and allow public safety entities to benefit from commercial economies of scale that otherwise would not exist. Before the D block is auctioned, it must be clear that any D block licensee(s) will be required to provide roaming and WPS-like priority access with reasonable compensation.

  Second, it is critical to develop commercial devices that can operate across 3GPP Band 14 in its entirety. (Band 14 in the 700 MHz band includes the D block and the public safety broadband spectrum.) Accordingly, the FCC should require the D block licensee(s), and potentially other 700 MHz commercial licensees, to develop and offer devices capable of providing service using all 700 MHz Band 14 spectrum and identify a path toward the large-scale production of such devices. Commercial devices should allow the public safety community access to better and less expensive options for use in the public safety spectrum, and will facilitate access to spectrum blocks where the D block licensee and the public safety licensee enter into a shared network partnership. The FCC should explore other ways to encourage the deployment of public safety devices that transmit across the entire broadband portion of the 700 MHz band (i.e., Band 12, Band 13, Band 14 and Band 17).
- *Liability protection for commercial partners.* A federal statute provides wireless, Voice over Internet Protocol (VoIP) and other emergency communications providers with immunity or liability protection for carriage of public safety communications that is not less than the immunity or liability protection given to local exchange carriers.[9] Commercial licensees should have similar liability protection for public safety communications when, for example, public safety licensees are roaming or using priority access on commercial networks or on shared networks supporting both commercial and public safety communications.
- *Leveraging purchasing power.* The FCC, working with other federal agencies, should explore other cost-saving measures for the buildout of public safety broadband networks. ERIC and DHS should work with the General Services Administration (GSA) to provide rate schedules that public safety entities can use to access commercial nationwide broadband networks and to obtain equipment for their networks. This would generate immediate cost savings and provide an important cost benchmark. In addition, state, Tribal and local governments can help lower costs. Infrastructure sharing can also reinforce network reliability and service continuity among commercial networks, particularly carriers entering into incentive-based partnerships with public safety organizations.

ERIC

The FCC should create ERIC under the umbrella of the Public Safety and Homeland Security Bureau immediately. ERIC will develop common standards for interoperability and operating procedures to be used by the public safety entities licensed to construct, operate and use this nationwide network. To establish a common vision, ERIC must exist before any licensees begin construction of such a network. This will ensure that government, public safety and the communications industry move away from creating and supporting fragmented public safety networks for broadband wireless communications.[10]

ERIC will establish a baseline for the seamless exchange of public safety wireless broadband communications on a nationwide, interoperable basis from the start of the network's development. This is crucial to allow responders from varying jurisdictions and disciplines to communicate with one another when they converge at an emergency, or when incidents span several jurisdictions. Similarly, first responders must have access to common applications in any situation or location.[11] To ensure success and leverage existing expertise, ERIC should be chartered to work closely with DHS's Office of Emergency Communications (OEC). Close coordination will enable ERIC to complement OEC's mission of creating standard operating procedures and governance to ensure that public safety communications flow over a seamless network. ERIC also should have a public safety advisory body to ensure appropriate consultation.[12]

The FCC's FY2011 budget proposes $1.5 million in funding to establish ERIC and support initial staffing requirements. As ERIC and the proposed broadband networks mature, about $5.5 million will be necessary each year starting in FY2012 for ERIC to be fully functional.[13] These additional funds will allow the FCC to partner with the National Institute of Standards and Technology (NIST) to develop appropriate standards and to maintain ERIC's expertise. The funds will also ensure adequate staffing to address the three core functions of ERIC: network engineering, network technical operations and network governance. In addition, Congress should consider providing DHS $1 million of public funding in FY2011, as proposed in its budget, and each year thereafter. The funding will help DHS to coordinate ERIC with OEC and relevant DHS entities, and enhance OEC outreach to Tribal, state and local agencies.

At a minimum, ERIC should:

- Adopt technical and operational requirements and procedures to ensure a nationwide level of interoperability; this should be implemented and enforced through FCC rules, license and lease conditions and grant conditions.
- Adopt and implement other enforceable technical, interoperability and operational requirements and procedures to address, at a minimum, operability, roaming, priority access, gateway functions and interfaces and interconnectivity of public safety broadband networks.
- Adopt authentication and encryption requirements for common public safety broadband applications and network use.
- Coordinate the interoperability framework of regulations, license requirements, grant conditions and technical standards with other entities (e.g., the public safety broadband licensee(s), DHS, NIST and the National Telecommunications and Information Administration).

ERIC should also work with DHS and the public safety community to ensure that the public safety broadband network and public safety narrowband wireless networks can communicate with one another seamlessly. ERIC's public safety advisory committee[14] will provide input from the public safety community on ERIC's proposed actions.

ERIC should work with NIST's Public Safety Communications Research Program to ensure that it collaborates in its work on research, development, testing, evaluation and standards with both the public safety community and industry. No federal laboratory facilities exist to independently test and demonstrate public safety 700 MHz broadband technologies. Creating a neutral host facility will allow all stakeholders to work together to develop a nationwide seamless public safety wireless broadband network and ensure that commercial broadband standards can meet public safety's specific requirements. This will help make networks and equipment compatible for public safety use.

NIST has announced that it is moving forward with development of a demonstration 700 MHz public safety broadband network in FY2010. Congress should consider allocating long-term public funding to continue this and other programs that support the new public safety network.

Grant Program

Development of a nationwide public safety broadband network through incentive-based partnerships will make Americans safer and more secure.[15] A grant program will give public safety its own "hardened" broadband wireless access network; ensure that the most vulnerable areas of the United States have the coverage they require; provide public safety with additional capacity and resiliency via access to nearby commercial spectrum; ensure that the emergency response community has the tools it requires; and optimize the effective use of resources.

As shown in Exhibit 16-B, a multi-pronged approach will provide public safety with greater dependability, capacity and cost savings. First, the hardened network will provide reliable service throughout a wide area. Second, since emergency responders will be able to roam on commercial networks, capacity

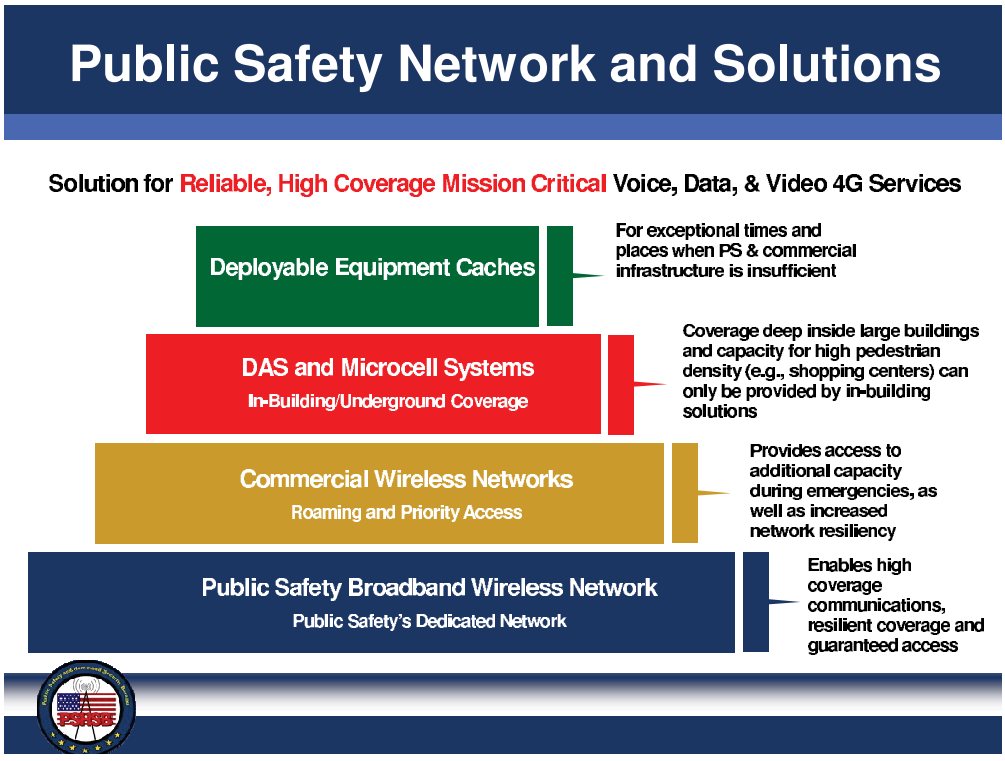
and resiliency will improve, at a reasonable cost. Third, localized coverage will improve through the use of fixed microcells—like those that provide indoor coverage in skyscrapers—and mobile microcells, which can be placed in fire trucks, police cars and ambulances. Fourth, equipment can be retrieved from caches and used during a disaster when infrastructure is destroyed or insufficient or unavailable. Grants to support the public safety broadband network should be distributed by a single agency to streamline operations, reduce costs and ensure that grants are made in a consistent manner. The grants should only fund projects that comply with ERIC requirements and should be made for the following four purposes:

- Construction of a public safety 700 MHz broadband network that involves partnerships and uses commercial infrastructure, the public safety infrastructure or both through incentive-based partnerships.
- Coverage of the rural areas within the network's geography.
- Hardening of the existing commercial network and new sites that operate as part of the public safety network (including covering non-recurring engineering costs for priority broadband wireless).[16]
- Development of an inventory of deployable capability for the 700 MHz public safety band.

A single grant-making agency, in coordination with ERIC, should structure the funding to ensure the network is built efficiently. The grant-making agency should have flexibility to limit the time that a grant recipient has to spend any granted funds. It should also ensure that the money spent is accounted for through reporting and auditing requirements. The grant-making agency should encourage grant recipients to enter into infrastructure-sharing agreements, where appropriate, with entities deploying broadband networks with support from other grant programs. Such arrangements should be reviewed annually, and any savings they generate should be taken into account when allocating funds for each program.

The public safety broadband network requires a substantial investment. Using a 99% population coverage model,[17] deployment of this network will require as much as $6.5 billion in capital expenditure in 2010 dollars over a 10-year period, which can be reduced through efficiency measures such as state and local programs and USF.[18] Initial public funding for the capital requirement should commence in a timely manner to enable the public safety network to benefit from the planned build-outs of the private 4G wireless broadband networks, which are scheduled to begin in 2010. Congress should consider providing the bulk of these funds in the second to fifth years of the network's construction.

Exhibit 16-B: Public Safety Network and Solutions



Ongoing costs, including operating expense and appropriate network improvement costs are expected to rise from zero at the beginning of FY2011 to a peak of as much as $1.3 billion per year in year 10 of the capital build program, following a substantial ramp-up that coincides with the network's expansion.[19]

The total present value of the capital expenditure and ongoing costs over the next 10 years is approximately $12–16 billion. State and local governments could contribute funds to cover some of these costs, and there may be additional cost-saving methods that reduce this estimate—such as sharing federal infrastructure, working with utilities, or use of state and local tower sites to improve coverage. This undertaking is also expected to produce a significant number of long-term U.S. jobs.[20]

It is essential that the United States establish a long-term, sustainable and adequate funding mechanism to help pay for the operation, maintenance and upgrade of the public safety broadband network. America's safety depends on it. Congress should consider creating such a funding mechanism in FY2011, but in any event, no later than FY2012. Recognizing that Americans will obtain substantial benefits from the creation of this network, imposing a minimal public safety fee on all U.S. broadband users would be a fair, sustainable and reasonable funding mechanism. The fee should be sufficient to support the operation and evolution of the public safety broadband network.

It is essential that the public safety community has the funds to operate, maintain and improve this network. All U.S. broadband users will benefit from this network. Spreading nominal costs among them will ensure that this country's emergency responders have access to critical communications capabilities when and where they need them.[21]

Congress should consider authorizing the FCC to impose or require the imposition of such a fee or other funding means. Congress should also consider enabling FCC the to implement or authorize mechanisms to collect, manage, audit and support the grant-making agency's disbursement of these funds. Receipts would fund the grant-making agency's program for public safety broadband operations and evolution. Strict conditions must be established to prohibit any diversion of these funds by state and local governments, and require adherence to ERIC-developed standards. The grant-making agency should be authorized to determine how to best allocate these funds to ensure an appropriate balance among urban, suburban and rural users and to require grant recipients to account for the funds they receive. And it should distribute the funds in a way that also enables the evolution of the network.

Existing Programs

In emergencies, the federal government uses an FCC-developed system called Project Roll Call to determine the operational status of wireless and broadcast communications (including public safety communications) and to help emergency managers restore operations when necessary. However, the system is not designed to operate in a 700 MHz broadband spectrum environment. Deployment of a new broadband public safety network will require a redesign of Project Roll Call and the procurement of new equipment to operate over the new spectrum. These efforts will give the federal government the capability it needs to rapidly restore public safety broadband communications in a disaster or emergency. Accordingly, Congress should consider providing an additional $6.9 million no later than FY 2012—and $1.9 million of public funding on a recurring annual basis—to the FCC for the design and acquisition of enhanced Roll Call systems.

Exhibit 16-C: Selection of Proposed Broadband Applications and Services for the Public Safety Broadband Network

Public Safety Spectrum Trust	• Remote access to criminal databases • High-speed file downloads • Distribution of surveillance video feeds to on-scene personnel
The National Association of State EMS Officials	• Medical-quality video • Multiple vital signs transmission • Real-time resource tracking (e.g., of ambulances) • Secure transmission of patient records
National Public Safety Telecommunications Council	• Intelligence gathering • Automated inspections • Environmental monitoring • Traffic management
AT&T	• Location-based services • Messaging • Virtual private networking
Telcordia	• Real-time command and control • Logistics and decision support
District of Columbia	• Real-time identity management and credentialing • Interoperability with computer-aided dispatch systems, emergency operation centers and voice systems

RECOMMENDATION 16.2: Survey public safety broadband wireless mobile infrastructure and devices.

There is a lack of detailed information about state and local deployments of public safety broadband networks, infrastructure and equipment. FEMA, working with Regional Emergency Communications Coordination working groups, periodically collects data on narrowband systems .[22] But there is no systematic study of public safety wireless broadband communications networks. Documentation of deployment and use of broadband by the state, Tribal and local public safety community, including the status of interoperability, will help in evaluating programs that support this technology.

Accordingly, Congress should consider providing public funding of $3.75 million per year for three years (for a total of $11.3 million) to allow FEMA to expand its data collection and survey efforts with states and territories. Providing federal, Tribal, state and local governments with up-to-date information on public safety broadband capabilities can help target grants to fill broadband gaps.[23]

RECOMMENDATION 16.3: Ensure that broadband satellite service is a part of any emergency preparedness program.

Technical factors can affect broadband service during disasters,but it is vital that broadband networks operate reliably and have redundant capabilities in an emergency. A way to ensure this is to use existing broadband mobile and fixed satellite services in an affected area in the event of a disaster or crisis. Satellites can serve as a communications option and a critical source of redundancy, particularly when terrestrial infrastructure is unavailable. Satellite services may be even more important as a method of communication in the first few hours or days of a disaster, should terrestrial-based services be damaged or destroyed—providing unique value for public safety purposes. Already, several state, local and federal agencies use broadband satellite service applications for public health, continuity of government and disaster preparedness activities.[24]

Federal agencies should recommend the use of broadband fixed and mobile satellite service for emergency preparedness and response activities, as well as for national security, homeland security, continuity and crisis management.[25] These recommendations should be issued when the agencies offer emergency preparedness and response information guidelines to the emergency response community, or when they develop plans and programs on emergency response. The U.S. Government Accountability Office (GAO) should issue a report on the current and future capability of satellite broadband to provide necessary service during an emergency.

RECOMMENDATION 16.4: Preserve broadband communications during emergencies.

Current law bars for-profit entities, such as hospitals, broadcasters and service providers, from receiving federal assistance to maintain or restore communications—including broadband and broadcast services—immediately following a disaster. However, certain for-profit communications entities provide vital services that ensure public safety. Hospitals, for example, provide public health information, while broadcasters distribute important information and warn the public of impending dangers. The inability to maintain or restore broadband service may prevent hospitals and public health officials from sharing time-sensitive information. Loss of power or broadband connectivity also could prevent broadcasters from distributing health information to the public on a timely basis.[26] Without federal efforts to maintain and quickly restore broadband and broadcast services, the most vulnerable residents could be cut off from essential services such as NG 911, alerts and warnings, including Emergency Alert System (EAS) messages.

Accordingly, Congress should consider amending the Stafford Act to permit limited federal assistance during a disaster to private, for-profit entities—including health care providers, broadcasters and communications service providers—to maintain or restore public safety-related critical communications services (e.g., public warning and alerts, law enforcement, fire, medical, search and rescue, PSAPs and other emergency services) during a major disaster. The Federal Coordinating Officer or Federal Resource Coordinator at the Joint Field Office (JFO)—or, prior to establishment of a JFO, the Operations Section Chief at the National Response Coordination Center—should be authorized to decide whether to grant requests for such federal assistance.[27] To prevent abuse, requests should be granted only for services related to operational issues and only for a limited duration, such as 30 days. [28] These statutory and regulatory changes should be made effective prior to the start of the 2010 hurricane season in June, because of the possibility of frequent and large-scale weather-related disasters.

16.2 PROMOTING CYBERSECURITY AND PROTECTING CRITICAL INFRASTRUCTURE

Improving Cybersecurity

Communications providers have experienced frequent attacks on critical Internet infrastructure. A variety of state and non-state entities has demonstrated the ability to steal, alter or destroy data and to manipulate or control systems designed to ensure the

functioning of portions of our critical infrastructure. Additional safeguards may be necessary to protect our nation's commercial communications infrastructure from cyberattack. Such safeguards could promote confidence in the safety and reliability of broadband communications and spur adoption.

RECOMMENDATION 16.5: The FCC should issue a cybersecurity roadmap.

Admiral Mike McConnell, former Director of National Intelligence, said recently that "the United States is fighting a cyber-war today, and we are losing."[29] He noted that "to the extent that the sprawling U.S. economy inhabits a common physical space, it is in our communications networks."[30] The country needs a clear strategy for securing the vital communications networks upon which critical infrastructure and public safety communications rely. Within 180 days of the release of this plan, the FCC should issue, in coordination with the Executive Branch, a roadmap to address cybersecurity. The FCC roadmap should identify the five most critical cybersecurity threats to the communications infrastructure and its end users. The roadmap should establish a two-year plan, including milestones, for the FCC to address these threats.

RECOMMENDATION 16.6: The FCC should expand its outage reporting requirements to broadband service providers.

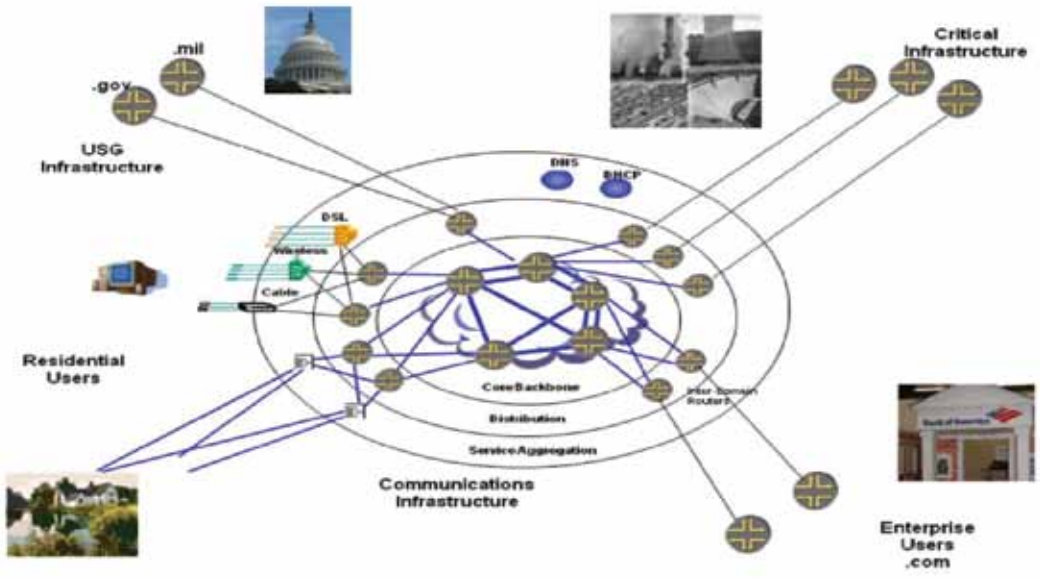
Today the FCC currently does not regularly collect outage information when broadband service providers experience network outages. This lack of data limits our understanding of network operations and of how to prevent future outages. The FCC should initiate a proceeding to extend FCC Part 4 outage reporting rules to broadband Internet service providers (ISPs) and interconnected VoIP providers. Such reports will allow the FCC, other federal agencies and, as appropriate, service providers to analyze information on outages affecting IP-based networks. The information also will help prevent future outages and ensure a better response to actual outages.
The timely and disciplined reporting of network outages will help protect broadband communications networks from cyberattacks, by improving the FCC's understanding of the causes and how to recover. This will help improve cybersecurity and promote confidence in the safety and reliability of broadband communications.[31]

RECOMMENDATION 16.7: The FCC should create a voluntary cybersecurity certification program.

Many Internet users apparently do not consider cybersecurity a priority. Nearly half of all businesses in the 2009 Global State of Information Security Study reported that they are cutting budgets for information security initiatives. A 2008 Data Breach Investigations Report concluded that 87% of cyber breaches could have been avoided if reasonable security controls had been in place.[32] The FCC should explore how to encourage voluntary efforts to improve cybersecurity.

The FCC should begin a proceeding to establish a voluntary cybersecurity certification system that creates market incentives for communications service providers to upgrade their network cybersecurity. The FCC should examine additional voluntary incentives that could improve cybersecurity as and improve education about cybersecurity issues, and including international aspects of the issues. A voluntary cybersecurity certification program could promote more vigilant network security among market participants, increase the security of the nation's communications infrastructure and offer end-users more complete information about their providers'

Exhibit 16-D :
The Cyber World



cybersecurity practices. In this proceeding, the FCC should consider all measures that will promote confidence in the safety and reliability of broadband communications. [33]

RECOMMENDATION 16.8: The FCC and the Department of Homeland Security (DHS) should create a cybersecurity information reporting system (CIRS).

The FCC, other government partners and ISPs lack "situational awareness" to allow them to respond in a coordinated, decisive fashion to cyber attacks on communications infrastructure. The FCC and DHS's Office of Cybersecurity and Communications together should develop an IP network CIRS to accompany the existing Disaster Information Reporting System. CIRS will be an invaluable tool for monitoring cybersecurity and providing decisive responses to cyberattacks.

CIRS should be designed to disseminate information rapidly to participating providers during major cyber events. CIRS should be crafted as a real-time voluntary monitoring system for cyber events affecting the communications infrastructure. The FCC should act as a trusted facilitator to ensure any sharing is reciprocated and that the system is structured so ISP proprietary information remains confidential.

RECOMMENDATION 16.9: The FCC should expand its international participation and outreach.

The FCC should increase its participation in domestic and international fora addressing international cybersecurity activities and issues. It should also engage in dialogues and partnerships with regulatory authorities addressing cybersecurity matters in other countries. This should include outreach to foreign communications regulators and international organizations about elements of the National Broadband Plan (see Chapter 4 which discusses international outreach). The FCC should also continue to review other nations' and organizations' cybersecurity activities so it is better aware of those activities as they relate to U.S. domestic policies. And it should continue to participate in domestic initiatives that relate to cybersecurity activities in the international arena.

Critical Infrastructure Survivability

RECOMMENDATION 16.10: The FCC should explore network resilience and preparedness.

Simultaneous failure of or damage to several IP network facilities or routers could halt traffic between major metropolitan areas or between national security and public safety offices. Because many companies colocate equipment, damage to certain buildings could affect a large amount of broadband traffic, including NG 911 communications. The FCC should begin an inquiry into the resilience of broadband networks under a set of physical failures—either malicious or non-malicious—and under severe overload. This will allow the FCC to assess the ability of next-generation public safety communications systems to withstand direct attacks and to determine if any actions should be taken in this regard.

This proceeding should also examine commercial networks' preparedness to withstand overloads that may occur during extraordinary events such as bioterrorism attacks or pandemics. DHS has developed pandemic preparedness best practices for network service providers, but adherence to these voluntary standards is not tracked. For example, a surge in residential broadband network use during a pandemic or other disaster could hinder network performance for critical users and applications by hindering the flow of time-sensitive medical and public health information over public networks. This proceeding will give the FCC insight into pandemic preparedness in commercial broadband networks. In addition, it will yield important information about the susceptibility of such networks to severe overloads and how network congestion on residential-access networks—particularly in the "last mile"—may undermine public safety communications and 911 access during a pandemic or other large-scale event.[34]

RECOMMENDATION 16.11: The FCC and the National Communications System (NCS) should create priority network access and routing for broadband communications.

Broadband users in the public safety community have no system of priority access and routing on broadband networks. Such a system is critical to protect time-sensitive, safety-of-life information from loss or delay due to network congestion. While technical work is under way to allow the creation of such a system, no corresponding set of FCC rules exists to support it. The FCC and the National Communications System (NCS) should leverage their experience with the Government Emergency Telecommunications Service (GETS) and the WPS to jointly develop a system of priority network access and traffic routing for national security/emergency preparedness (NS/EP) users on broadband communications networks. The Executive Branch should consider clarifying a structure for agency implementation and delineating responsibilities and key milestones; the order should be consistent with national policies already in existing presidential documents.The FCC and NCS should jointly manage this program.

RECOMMENDATION 16.12: The FCC should explore standards for broadband communications reliability and resiliency.

For years, communications networks were designed and deployed to achieve "carrier-class" reliability. As the communications infrastructure migrates from older technologies to broadband technology, critical communications services will be

carried over a communications network that may or may not be built to these high standards. The potential decline in service reliability is a concern for critical sectors, such as energy and public safety, and for consumers in general. The FCC should begin an inquiry proceeding to gain a better understanding of the reliability and resiliency standards being applied to broadband networks. The proceeding should examine the standards and practices applied to broadband infrastructure at all layers, from applications to facilities. Its objective should be to determine what action, if any, the FCC should take to bolster reliability of broadband infrastructure.

16.3 LEVERAGING BROADBAND TECHNOLOGIES TO ENHANCE EMERGENCY COMMUNICATIONS WITH THE PUBLIC

The Move to Next Generation 911

The nation's 911 system is evolving toward supporting NG911, which will integrate the core functions and capabilities of Enhanced 911 (E911) while adding new 911 capabilities in multiple formats, such as texting, photos, video and e-mail. NG911 also will integrate entities involved in emergency response beyond the PSAP (see Exhibit 16-E.). This will vastly improve the quality and speed of response, giving all callers—including people with disabilities—equal service. The possibility of sending video and photographs to the PSAP will transcend language barriers and provide eyewitness-quality information to give first responders the most relevant information at the scene of an emergency. NG911 will provide a more interoperable and integrated emergency response capability for PSAPs, first responders, hospitals and other emergency response professionals.

The four fundamental purposes of NG911 are to:

- Replace the E911 system while retaining its core functions, such as automatic location information and automatic number identification.
- Add capabilities to support 911 access in multiple formats for all types of originating service providers, application developers and device manufacturers.
- Increase system flexibility, redundancy and efficiency for PSAPs and 911 governing authorities.
- Add capabilities to integrate and interoperate with entities involved in emergency response beyond the PSAP.

Broadband will make it possible for PSAPs to push and pull video, images, medical information, environmental

Exhibit 16-E:
Call Flow in NG911[35]

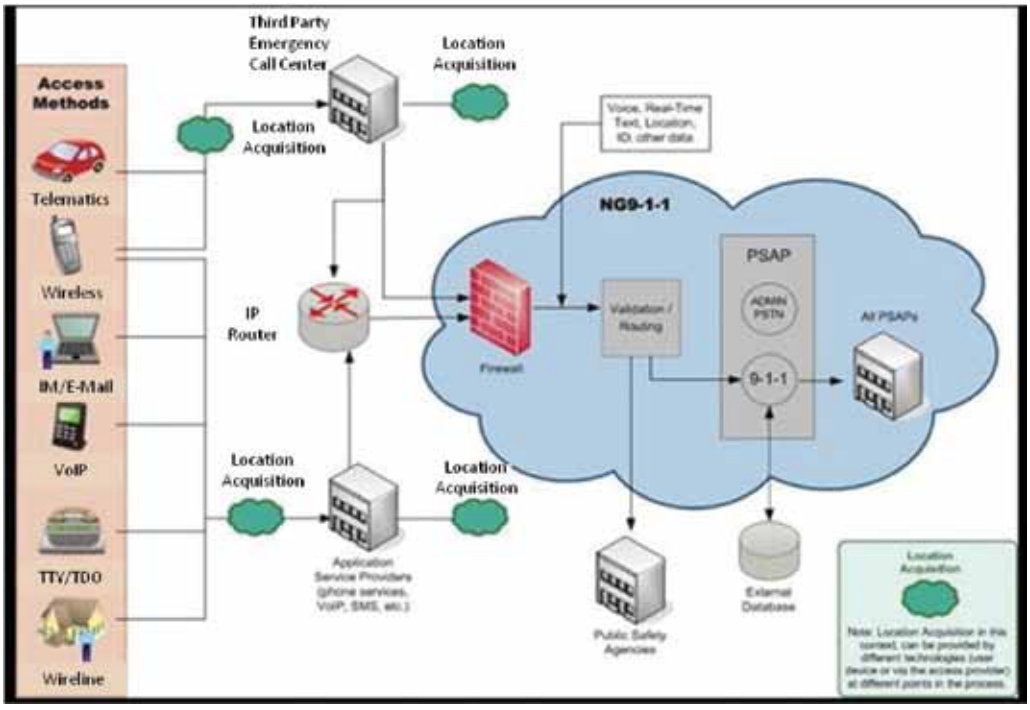
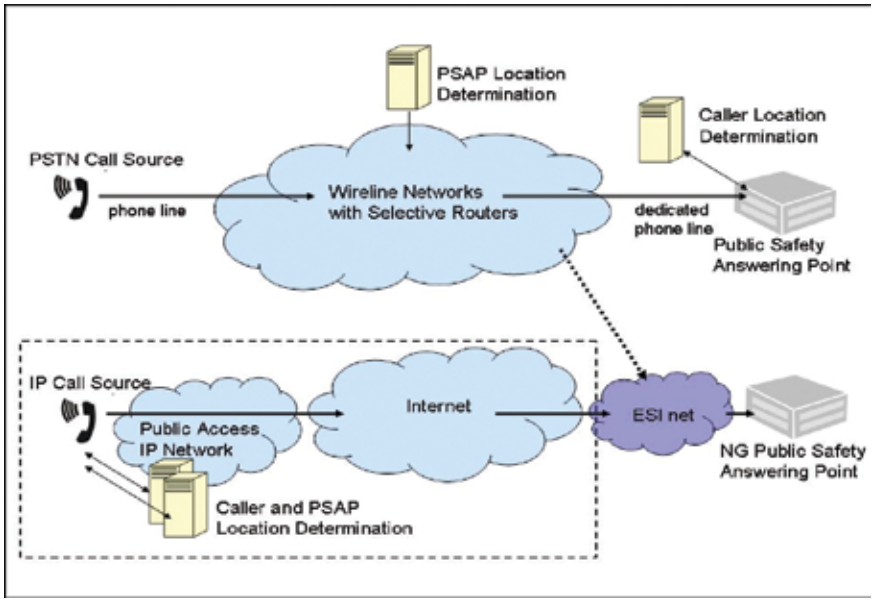


Exhibit 16-F:
NG911 Will Enable the Public to Access 911 Through Text Messaging (SMS) and Other Formats

Exhibit 16-G:
Physical Architectures of Current and Next-Generation 911



sensor transmissions and a host of other data through shared databases and networks. This will make it easier for the public—including persons with disabilities—to access 911 services. Users will be able to transmit voice, text or images to PSAPs from a variety of broadband-capable devices.

Using Broadband to Bridge the Gap to NG911

Many in the public safety community lack access to broadband services.[36] Some PSAPs are located in areas where broadband communications are unavailable.[37] Many PSAPs cannot afford broadband connectivity, and existing grant programs are not focused on long-term funding activities. Further, regulatory roadblocks have hindered NG911 deployment. A more efficient transition needs to be developed to support these services.

The transition from the legacy 911 system to NG911 has begun. Public safety and industry standards organizations have reached a consensus on NG911 technical architecture to meet demands posed by new forms of technology and methods of communication. The U.S. Department of Transportation (DOT) has published a transition plan for NG911 migration.[38] Several states and localities have begun deploying NG911. At least one ongoing live test of 911 texting is underway[39] (see Exhibit 16-F).

Yet financial and regulatory barriers hinder NG911 implementation. Grant programs that support NG911 are uncoordinated and limited in scope. Inconsistent, overlapping and outdated state and federal regulations have slowed NG911 development.

BOX 16-2:

Iowa 911 Call Center Becomes First to Accept Texts[42]

An emergency call center in Black Hawk County, Iowa, became the first in the nation to accept text messages sent to "911" in August 2009. "I think there's a need to get out front and get this technology available," Black Hawk County police chief Thomas Jennings told the Associated Press.

Black Hawk County's system is designed so people with speech and hearing impediments can text 911 for emergency services. It eliminates the cumbersome process of having a deaf person using a keyboard to write a message, which is then delivered via a relay center to the operator answering the call. An added advantage is that 911 operators can text back.

While voice communication is still the primary method for 911 communications, this new wave of Next Generation 911 capability is just one example of the way the nation is modernizing its 911 system to better serve the public.

It is critical that the NG911 system is developed in a way that most effectively ensures Americans can access 911 systems anytime and anyplace. (see Exhibit 16-G for differences between the architecture of current legacy 911 and NG911 systems.) Further, the NG911 system must be able to quickly communicate caller-generated information to first responders. U.S. policy on NG911 should focus on fosteringrapid transition from analog, voice-centric 911 and emergency communications systems to a broadband-enabled, IP-based emergency services model.

RECOMMENDATION 16.13: The National Highway Traffic Safety Administration (NHTSA) should prepare a report to identify the costs of deploying a nationwide NG911 System and recommend that Congress allocate public funding.

The lack of coordinated funding is a significant roadblock for NG911 deployment. Several agencies administer existing grant and loan programs without any central coordination or uniform criteria.[40] Moreover, limited information has been developed on the potential cost of NG911 implementation. Though DOT estimated in mid-2008 that the total cost of implementing and operating a nationwide NG911 system over the next 20 years would be $82 to $87 billion,[41] the country requires a more detailed and targeted report to help Congress develop a grant program. A NHTSA analysis should determine detailed costs for specific NG911 requirements and specifications, and specify how costs would be broken out geographically or allocated among PSAPs, broadband service providers and third-party providers of NG911 services. The NHTSA report should also address the current state of NG911 readiness among PSAPs and how differences in PSAP access to broadband across the country may affect costs.

Congress should consider providing public funding for NHTSA to analyze the costs of deploying a nationwide NG911 system. The report should be completed by Dec. 1, 2011. It should include a technical analysis and cost study of different delivery platforms—such as wireline, wireless and satellite—and an assessment of the architectural characteristics, feasibility and limitations of NG911 delivery. The report also should include an analysis of the needs of persons with disabilities and should identify standards and protocols for NG911 and for incorporating VoIP and "Real Time Text" standards.[43] The report should be a resource for Congress as it considers creating a coordinated, long-term funding mechanism for NG911 deployment and operation, accessibility, application development, equipment procurement and training. This analysis is essential to identify funding requirements for the implementation of NG911.

RECOMMENDATION 16.14: Congress should consider enacting of federal NG911 regulatory framework.

Federal and state regulations that focus on legacy 911 systems have hampered NG911 deployment.[44] Many rules were written when the technological capabilities of NG911 did not exist.[45] Congress should consider establishing a federal legal and regulatory framework for development of NG911 and the transition from legacy 911 to NG911 networks. This framework should remove jurisdictional barriers and inconsistent legacy regulations and provide legal mechanisms to ensure efficient and accurate transmission of 911 caller information to emergency response agencies. Without such a comprehensive framework and a funding mechanism, it is unlikely all Americans will receive the benefits of NG911 in the near term.

The legislation should recognize existing state authority over 911 services but require states to remove regulatory roadblocks to NG911 development. It should also give the FCC the authority to implement a NG911 federal regulatory framework, eliminate outdated 911 regulations at the federal level and preempt inconsistent state regulations. This legislation should be coordinated with the NHTSA report to ensure federal regulation of NG911 is consistent.

Congress should also consider steps to curtail Tribal, state and local use of 911 funds for purposes other than 911. In the FCC's "Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges" for the year ending Dec. 31, 2008, some states reported that 911/E911 funds collected at the state level are or may be used, at least in part, to support non-911 and E911 programs.

Congress should also consider amending and reauthorizing the ENHANCE 911 Act and restoring the E911 Implementation Coordination Office (ICO) with appropriate funding. ICO can build upon its prior work with wireless and IP-enabled 911 services and help ensure NG911 is deployed in an interoperable and reliable fashion.

RECOMMENDATION 16.15: The FCC should address IP-based NG911 communications devices, applications and services.

The FCC is considering changes to its location accuracy requirements and the possible extension of Automatic Location Identification (ALI) requirements to interconnected VoIP services.[46] The FCC should expand this proceeding to explore how NG911 may affect location accuracy and ALI.

The current 911 system will also need to be re-evaluated as broadband-based communications continue to proliferate. The 911 system mainly provides a voice-centric communications platform between the public and 911 operators. However, the deployment of different types of communications, devices, applications and services has meant consumers are changing their expectations about how they can access 911. Many consumers, for example, already have come to expect they may send non-voice communications, such as short text messages and multimedia messages, to PSAPs. But PSAPs typically cannot receive such communications. The national strategy for NG911 deployment should be designed to meet future consumer expectations.

New broadband-based devices and applications may not offer the traditional voice and "call" capabilities that wireless or VoIP phones do today. Thus, consumers may assume they can reach PSAPs via various IP-based communications modes. Non-voice methods of communicating with 911 would have the added benefit of promoting accessibility to 911 for non-English-speaking persons and persons with disabilities. Thus, the FCC should initiate an additional proceeding to address how NG911 can accommodate communications technologies, networks and architectures beyond traditional voice-centric devices. It should also explore how public expectations may evolve in terms of the communications platforms the public would rely upon to request emergency services.

Moving Toward Next-Generation Alerting

Building on today's emergency alerting technology, FEMA has taken steps to develop an Integrated Public Alert and Warning System (IPAWS) that will lead to a next-generation public alert and warning system.[48] The IPAWS vision is to build and maintain an effective, reliable, integrated, flexible and comprehensive system that allows Americans to receive alert and warning information through as many communication pathways as possible.[49] But in a September 2009 report, GAO identified a number of challenges with IPAWS implementation, including some related to the inclusion of new technologies,[50] stakeholder coordination[51] and technical issues.[52] States and localities need additional resources to upgrade their alerting operations to effectively access IPAWS.

BOX 16-3:

Emergency Alert System Saves Lives in American Samoa[47]

On Sept. 29, 2009, an 8.1 magnitude earthquake triggered a tsunami in American Samoa—the biggest earthquake of that year. KKHJ, the primary station in American Samoa's Emergency Alert System, issued 2 EAS alerts—one after the earthquake hit and a second when waters in Pago Pago Harbor began to rise. This EAS alert warned residents to evacuate the area. Upon receiving the alert, a pastor from the village of Amanave rang his church bells, providing a further warning to locals to evacuate the area. Although more than 180 people perished in the earthquake and tsunami, the early warning system is credited with saving lives.

Further, the federal government should disseminate information about IPAWS development and deployment.

RECOMMENDATION 16.16: The FCC should launch a comprehensive next-generation alert system inquiry.

The FCC should quickly begin a proceeding exploring all issues for developing a multiple-platform, redundant next-generation alert system. Next-generation alerting should include delivery of emergency alerts throughout the nation via broadband. The inquiry should consider Emergency Alert System (EAS) and Commercial Mobile Alert Service (CMAS) developments, as well as FEMA's development of IPAWS. It also should consider all potential multiplatform technologies, including the use of emergency alerts via video programming on the Internet. The inquiry should determine how best to ensure all Americans can receive timely and accurate alerts, warnings and critical information about emergencies regardless of the communications technologies used.

The FCC has not yet begun a wide-ranging inquiry into next-generation alerting. Such an inquiry can bridge the gap from the current EAS and CMAS systems to a comprehensive next-generation alerting system by detailing an implementation strategy. Such a proceeding should be initiated.

Next-generation technologies will transform the information delivery capabilities of both EAS and CMAS. They can also increase the effectiveness of alerts during emergencies. Emergency managers could provide alerts to communities now served poorly—such as persons with disabilities and non-English speakers—and provide improved alert file "trails" containing valuable information, such as full-motion videos of radar-tracked storm systems. Emergency alerts in Internet video format would allow emergency alert originators to reach people who are not, at the time, listening to broadcast radio and television or other current sources of alerts. Providing alternative methods for distributing emergency alerts to all Americans will save lives. However, the systems that assemble, manage and transmit alerts will need to be upgraded to accommodate broadband.

The system should alert the public of emergencies through all possible means of communications. In the event of a tornado, for example, alerts would be broadcast on local media outlets, sent to wireless and wireline phones within the affected area, posted on Internet feeds and websites sites, and issued through any other communication outlet serving the affected area. That would ensure the public is informed of an emergency and has the information it needs to protect itself. The FCC's inquiry should focus primarily on how to develop such a system.

FEMA's development of IPAWS should help ensure that a ubiquitous alert transmission system is available to accommodate multiple alert platforms and participation by all federal, state, Tribal, local and private sector alert stakeholders. There also needs to be a comprehensive evaluation of the ability of alert managers to participate in IPAWS when launched.

A comprehensive inquiry will allow the FCC to obtain input on the alerting system's future and to form a new regulatory framework for next-generation alerting. This inquiry should focus on the wide-ranging technical, legal and policy issues associated with this new multi-platform system. The proceeding should analyze the developing IPAWS architecture to evaluate the ability of IPAWS to support a broadband-based, next generation alert system. The inquiry also should examine the needs of state, Tribal and local emergency alert originators in utilizing the next-generation alerting system; what assistance, if any, the FCC and its federal partners should provide to address those needs; and what actions the FCC and federal partners should take to ensure the system's timely development and deployment.

RECOMMENDATION 16.17: The Executive Branch should clarify agency roles on the implementation and maintenance of a next-generation alert and warning system.

The Executive Branch through an interagency policy council or through a directive should take action by executive order, federal interagency policy committee or other formal means, to clarify the responsibilities of each federal agency in the implementation, maintenance and administration of next generation alerting systems. This action should also set milestones, benchmarks and necessary actions for implementation and establish a system of accountability among the federal agencies responsible for emergency alerting.

CHAPTER 16 ENDNOTES

1 Under this approach, for example, the public safety licensee(s) is afforded the flexibility to enter into agreements with commercial partners for construction and operation of their 700 MHz network.

2 Based on the results of the 2006 National Interoperability Baseline Survey, the 2007 UASI Tactical Interoperability scorecards, and 2008/2009 information provided by each state regarding its Statewide Communications Interoperability Plans, it is possible to estimate that a majority of the UASIs and states are at approximately an intermediate level of interoperability. *See generally* Dep't of Homeland Sec., 2006 National Interoperability Baseline Survey (2006), *available at* http://www.safecomprogram.gov/NR/rdonlyres/40E2381C-5D30-4C9C-AB81-9CBC2A478028/0/2006NationalInteroperabilityBaselineSurvey.pdf; Dep't Homeland Sec., Tactical Interoperable Communications Scorecards Summary Report and Findings (2007), *available at* http://www.dhs.gov/xlibrary/assets/grants-scorecard-report-010207.pdf; Dep't of Homeland Sec., National Summary of Statewide Communication Interoperability Plans (SCIPs) (2009), *available at* http://www.safecomprogram.gov/NR/rdonlyres/C6C0CD6A-0A15-4110-8BD4-B1D8545F0425/0/NationalSummaryofSCIPs_February2009.pdf. As set forth in the Goals of the National Emergency Communications Plan, DHS plans to assess each of the nation's 60 largest urban areas' ability to clearly achieve response-level communications by September 30, 2010, and will evaluate each of the more than 3,000 counties in the United States by September 30, 2011. *See* Dep't of Homeland Sec., National Emergency Communications Plan 6–7 (2008), *available at* http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf.

3 Eur. Telecomm. Standards Inst. [ETSI], Project MESA; *Technical Specification Group—System; System and Network Architecture*, at 20, ETSI TR 102 653 V3.1.1 (2007–2008), *available at* http://www.etsi.org/deliver/etsi_tr/102600_102699/102653/03.01.01_60/tr_102653v030101p.pdf.

4 *See Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229, Second Report and Order, 22 FCC Rcd 15289 (2007).

5 Comments submitted in the Commission's 700 MHz D block proceeding suggest a number of possible explanations. *See, e.g.*, Association of Public Safety Communications Officials-International, Inc. (APCO) Comments in re 700 MHz Third Further Notice (*Service Rules for the 698–746, 747–762 and 777–792 Bands; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, WT Docket No. 06-150, PS Docket No. 06-229, Third Further Notice of Proposed Rulemaking, 23 FCC Rcd 16661 (2008) (*700 MHz Third Further Notice*)), filed June 20, 2008, at 3; Verizon Wireless Comments in re 700 MHz Third Further Notice, filed June 20, 2008, at 2 .

6 The record includes proposals, for example, for public safety agencies to use existing core infrastructure while individuating end-user devices and other aspects of the edge network to meet public safety requirements, and also to employ satellite, aircraft or other technologies to extend coverage to rural areas. *See, e.g.*, Letter from Lucian Randolph, CEO, Planet TV Air-Tower Systems, to Marlene H. Dortch, Secretary, FCC GN Docket No. 09-51, (Nov. 12, 2009) (Planet TV Nov. 12, 2009 *Ex Parte*) at 9; Space Data Reply in re National Broadband Plan NOI, filed July 21, 2009, at 3; Iridium Satellite Comments in re National Broadband Plan NOI, filed June 8, 2009, at 4–5; MSS/ATC Coalition Comments in re National Broadband Plan NOI, filed June 8, 2009, at 5–6; Spacenet Inc. Comments in re National Broadband Plan NOI, filed June 8, 2009, at 9. The Commission should also explore how to best meet public safety requirements through a variety of means, including the use of commercial infrastructure to be procured by the public safety broadband licensee.

7 This serves the added purpose of allowing the public safety licensee(s) to leverage infrastructures that utilities might currently have. Therefore, access to utilities' towers and other structures may be part of any secondary usage program.

8 *See, e.g.*, APCO Comments in re NBP PN #8, (*Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan—NBP Public Notice #8*, GN Docket Nos. 09-47, 09-51, 09-137, PS Docket Nos. 06-229, 07-100, 07-114, WT Docket No. 06-150, CC Docket No. 94-102, WC Docket No. 05-196, Public Notice, 24 FCC Rcd 12136 (PSHSB 2009) (*NBP PN #8*)) filed Nov. 12, 2009, at 11; AT&T Comments in re NBP PN #8, filed Nov. 12, 2009, at 2; Verizon and Verizon Wireless Comments in re NBP PN #8, filed Nov. 12, 2009, at 6; Public Safety Spectrum Trust Comments in re *700 MHz Public Safety Broadband Networks Waiver PN (Public Safety and Homeland Security Bureau Seeks Comment on Petitions for Waiver to Deploy 700 MHz Public Safety Broadband Networks*, PS Docket No. 06-229, Public Notice, DA 09-1819 (rel. Aug. 4, 2009) (*700 MHz Public Safety Broadband Networks Waiver PN*) at 11.

9 *See* New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. No. 110-283, 122 Stat. 2620 (2008) (NET 911 Act) amending Wireless Communications and Public Safety Act of 1999, Pub.L. No. 106-81, 113 Stat. 1286 (1999) (Wireless 911 Act).

10 To the extent that other users are permitted on a public safety network, ERIC will also be responsible for working on establishing common priorities.

11 ERIC's mission can also be extended over time to serve other functions, such as coordinating PSAP access to the network and improving interoperability for mission critical voice.

12 The FCC should consider a membership comprised of representatives of state and local public safety agencies, public safety trade associations, the Public Safety Spectrum Trust, federal user groups, and SAFECOM. The FCC should also consider appropriate representation from industry representatives and representatives of equipment vendors and service providers. The FCC should also establish a federal partners coordinating committee that includes DHS, the Department of Justice, NIST and the National Telecommunications and Information Administration (NTIA) and that leverages the Emergency Communications Preparedness Center (ECPC).

13 This includes 20 new engineering and technical personnel, travel and office expenses, computing and simulation equipment and contracting with NIST for standards development and testing. Omnibus Broadband Initiative, The Public Safety Broadband Wireless Network (forthcoming) (OBI, The Public Safety Broadband Wireless Network).

14 This advisory committee should be made exempt from the Federal Advisory Committee Act. Secondly, Congress should ensure appropriate funding for ERIC to enable the FCC to pay for reasonable travel expenses of the public safety advisory committee members.

15 Under this model, public safety entities, as authorized by the FCC, should be allowed to select entities they want to partner with to construct and operate their networks, consistent with FCC, including ERIC, requirements.

16 Many state and local jurisdictions have enacted regulations requiring the installation of transmitters or other equipment within buildings to improve in-building coverage for public safety narrowband voice networks. State and local governments should consider implementing similar in-building coverage requirements for public safety broadband communications.

17 To achieve the 99% population coverage, externally mounted antennas are assumed for use in highly rural areas of the country.

18 The cost basis for this funding request will be released subsequently in an OBI, The Public Safety Broadband Wireless Network . These capital costs include leveraging approximately 41,600 commercially deployed sites, 3,200 rural sites (a blend of new and upgraded sites, with vehicles being mounted with externally deployed antennas), hardening of all sites, and providing deployable caches of equipment at the state and local level.

19 This figure is based on an annual RAN fee for managed services, additional costs for rural services and an annual OA&M including transport managed services fee. OBI, The Public Safety Broadband Wireless Network.

20 Most of these jobs will be in services and operations, while a smaller percentage will be in product development and manufacturing. OBI, The Public Safety Broadband Wireless Network.

21 Such a fee should be modest. Operating expenses for the first 2 years of network operation are estimated at $500 million.

22 *See* 6 U.S.C. § 575. This statute mandates the formation of RECC working groups, *id.* at § 575(a), and charges them with, among other duties, "assessing the survivability, sustainability and interoperability of local emergency communications systems." *Id.* at § 575(d)(1). This section does not direct the working groups to focus on broadband infrastructure.

23 These surveys should include information to be provided to ERIC on the current status of interoperability for the public safety broadband network.

CHAPTER 16 ENDNOTES

24 FCC, FCC Preparedness for Major Public Emergencies, Chairman's 30 Day Review (2009), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-293332A1.pdf.

25 *See* Letter from Diane Cornell, Vice President of Government Affairs, Inmarsat, to Marlene H. Dortch, Secretary, FCC, GN Docket Nos. 09-47, 09-51, 09-137, WC Docket No. 02-60 (Dec. 4, 2009) at 7.

26 *See* 47 U.S.C. § 5172(a)(1)(B); Office of the President, The Federal Response to Hurricane Katrina: Lessons Learned 58–59 (2006), *available at* http://georgewbush-whitehouse.archives.gov/reports/katrina-lessons-learned.pdf.

27 Ann Arnold, President, Tex. Ass'n of Broadcasters, Statement at FCC Summit: Lessons Learned: Hurricane Seasons 2008 (Dec. 11, 2008) *available at* http://www.fcc.gov/realaudio/mt121108.ram (1:00:35).

28 For-profit entities should be deemed eligible for assistance only when the need for their services exceeds the capabilities of the private sector and any relevant state, Tribal and local governments, or relates to an immediate threat to life and property, is critical to disaster response or community safety, or relates to essential federal recovery measures.

29 *See* Mike McConnell, Op.-Ed., *Mike McConnell on How to Win the Cyber-War We're Losing,* Wash. Post, Feb. 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html. (McConnell, How to Win the Cyber-War).

30 McConnell, *How to Win the Cyber-War*.

31 Steven Chabinsky, Deputy Ass't Director-Cyber Division, Fed. Bureau of Investigation (FBI), Testimony before the U.S. Senate Judiciary Committee, Subcommittee on Terrorism and Homeland Security (Nov. 17, 2009). The FBI considers the cyber threat against the nation to be "one of the greatest concerns of the 21st century." *Id.*

32 Verizon Business, 2008 Data Breach Investigations Report 2–3 (2008), *available at* http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

33 The Commission will have to allocate funding to obtain a vendor to develop audit criteria and to accredit third-party certification bodies. Congress should consider public funding for the FCC in its next budget and on an ongoing basis as required.

34 In fact, estimates of residential-access network capacity suggest that current networks can carry between 1/100 and 1/10 of their advertised per-user capacity. *See also* AT&T Comments in re National Broadband Plan NOI, filed June 8, 2009, at 67–69; Telcordia Comments in re National Broadband Plan NOI, filed June 8, 2009, at 19.

35 Research and Innovative Tech. Admin., Next Generation 911 Concept of Operations, Fig. 4-2, http://www.its.dot.gov/ng911/pubs/concept_operations.htm (last visited Feb. 15, 2010).

36 *See generally* NENA Comments in re NBP PN #8, filed Nov. 12, 2009.

37 PSST Comments in re NBP PN #8, filed Nov. 12, 2009, at 2.

38 U.S. Dep't of Transp., Next Generation 911 (NG9-1-1) System Initiative, Final Analysis of Cost, Value, and Risk (Mar. 5, 2009) (DOT NG911 Cost Study).

39 Intrado Comments in re NBP PN #8, filed Nov. 12, 2009, at 11.

40 For instance, through the 911 Access Program, the Rural Utilities Service provides low-interest loans to state and local governments, Indian tribes and other entities for facilities and equipment to improve 911 access in rural areas. Food, Conservation, and Energy Act of 2008, Pub. L. No. 110-246, §6107, 122 Stat. 1651, 1959 (2008); *see* E911 Grant Program, 74 Fed. Reg 29,967 (June 5, 2009).

41 U.S. Dep't of Transp., Next Generation 911 (NG9-1-1) System Initiative, Final Analysis of Cost, Value, and Risk (Mar. 5, 2009) (DOT NG911 Cost Study).

42 *See* Peter Svensson, *Iowa 911 Call Center Becomes First to Accept Texts*, ABC News, Aug. 5, 2009, http://abcnews.go.com/Technology/wireStory?id=8259735 .

43 Real-Time Text is a feature that allows users to see text as it is typed into a text interface.

44 NENA Comments in re NBP PN #8, filed Nov. 12, 2009, at 18–20.

45 *See* NENA Comments in re NBP PN #8, filed Nov. 12, 2009, at 18–20.

46 *See Wireless E911 Location Accuracy Requirements; Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems; 911 Requirements for IP-Enabled Service Providers*, PS Docket No. 07-114, CC Docket No. 94-102, WC Docket No. 05-196, Notice of Proposed Rulemaking, 22 FCC Rcd 10609 (2007).

47 *See* Federal Emergency Management Agency, Integrated Public Alert and Warning System (IPAWS): Success Stories, http://www.fema.gov/emergency/ipaws/successstories.shtm (last visited Mar. 5, 2010) (IPAWS Success Stories).

48 *See* Federal Emergency Management Agency, Integrated Public Alert and Warning System (IPAWS), http://www.fema.gov/emergency/ipaws/ (last visited Feb. 15, 2010).

49 GAO, Emergency Preparedness: Improved Planning and Coordination Necessary for Modernization and Integration of Public Alert and Warning System 14 (2009) (GAO Emergency Preparedness Report), *available at* http://www.gao.gov/new.items/d09834.pdf (noting that capabilities to distribute emergency alerts and warnings through e-mails, telephones, text message devices, cell phones, pagers and Internet-connected desktops have not been implemented).

50 GAO Emergency Preparedness Report at 20–24.

51 GAO Emergency Preparedness Report at 24–26. Challenges identified by GAO included lack of redundancy, gaps in coverage, systems integration, standards development, development of geo-targeted alerting and alerts for people with disabilities and those who do not speak English. In response to the report, the DHS agreed with GAO's recommendations for addressing these concerns and has begun to address many of these challenges. *See* Written Statement of Damon Penn, Assistant Administrator, FEMA before the Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings and Emergency Management, U.S. House of Representatives (Sept. 30, 2009), http://republicans.transportation.house.gov/Media/file/TestimonyEDPB/2009-09-30-Penn.pdf.

52 *See* Radio World, EAS Trigger Saved Lives in Samoa Tsunami (Sept. 20, 2009), http://www.radioworld.com/article/87954; Bill Hoffman, *Lucky To Be Alive After Tsunami Destroys Dream Resort*, New Zealand Herald, Oct. 1, 2009, *available at* http://www.nzherald.co.nz/american-samoa/news/article.cfm?l_id=500605&objectid=10600668.