EXECUTIVE BRANCH VIEWS ON PUBLIC SAFETY, HOMELAND SECURITY AND CYBERSECURITY ELEMENTS OF A NATIONAL BROADBAND PLAN

National Telecommunications and Information Administration
United States Department of Commerce
http://www.ntia.doc.gov

December 2009

TABLE OF CONTENTS

I. INTRODUCTION

The National Broadband Plan ("Plan")[1] is an historic opportunity for the Commission to set out a path forward for the next generation of public safety communications, Next Generation 911 (NG911) communications, and contribute to the ongoing efforts to address cybersecurity needs. In this document, representing the collective experience of key Executive Branch agencies, the Administration presents its vision for harnessing the power of the Internet and public-private partnerships to meet these critical national challenges. The Plan can chart a path that leverages the unique, innovative dynamics of the Internet in order to address important public safety, national security, and homeland defense priorities.

We are in an era of decentralized communications characterized by innovation at the edge of networks, facilitated by open-standards and lightweight protocols. Successful strategies for managing public safety, cybersecurity, and NG911 resources will begin by recognizing and leveraging the characteristics of the Internet that make cyberspace complex, incompatible with traditional command-and-control regulation, and innovative. Internet-driven innovation has fueled advances across the computer, communications and information marketplaces. Innovative information and communication services are enabled by a layered, open platform design strategy that facilitates the development of many diverse applications and services on top of open networks built using common technical standards. Public safety communications can benefit enormously from adoption of this new model.

To enable public safety, cybersecurity and NG911 innovation, the Plan should be guided by a layering of functions and activities. Figure 1 depicts the layered model and identifies the allocation of responsibilities in each layer that should guide any policy and regulatory activities related to the Internet with respect to important public safety, national security, and homeland defense priorities. At the Applications, Services, and Equipment layer, the private sector must lead in developing innovative solutions and implementation strategies. Standards and Protocol development activities guide the operation and evolution of broadband networks and enable the wide range of applications and services for public safety, homeland security, and cybersecurity purposes. The Telecommunications Network Core is comprised of networks operated by the Nation's communications infrastructure providers. Public policy, investment decisions, and service planning at all levels should be guided by this model.

---

[1] Public Notice, "Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan," NBP Public Notice #8, DA 09-2133, GN Docket No. 09-51, *et al.* (rel. Sept. 28, 2009) ("NBP Public Notice #8"), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-09-2133A1.pdf. The attached White Paper provides responses to questions posed in the Public Notice.

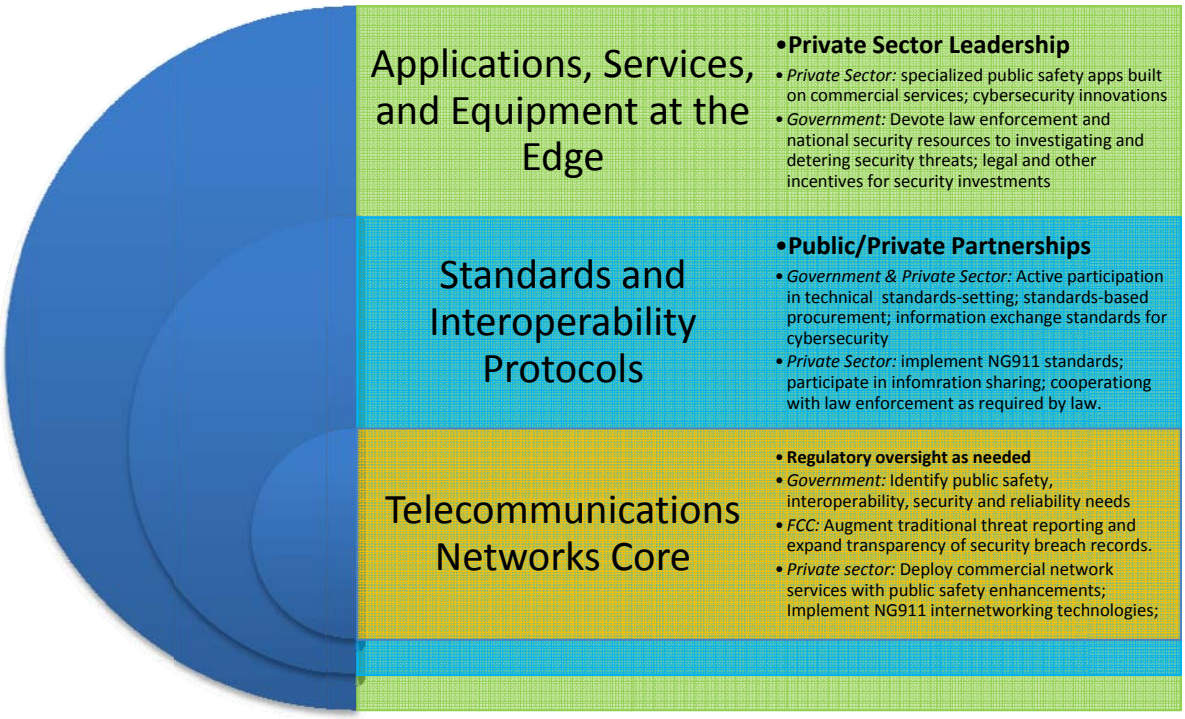

Figure 1 - Framework for Internet Development as It Relates to Public Safety, NG911 and Cybersecurity Responsibilities

II. PUBLIC SAFETY

Emergency responders envision near and long-term use of broadband applications that will improve situational awareness, provide real-time retrieval of critical data, and enhance collaborative decision-making. Along with these capabilities, the public safety community seeks seamless interoperability, robustness, reliability, and prioritization in a broadband network. To realize these goals completely, the public safety community must overcome a number of practical hurdles, ranging from the technical to the financial and regulatory. While continuing to work toward an optimal solution, the Federal Communications Commission ("Commission"), the Executive Branch agencies and their local, state and tribal counterparts, must address public safety's immediate broadband needs in ways that maximize the use of available resources. The Commission should explore whether public safety could effectively use existing core infrastructure, while individuating end user devices and other aspects of the network edge to meet unique public safety specifications. In so doing, the Commission should take into account the analysis of public safety communications' strengths and weaknesses conducted in the aftermath of 9-11 and Hurricane Katrina.[2]

[2] The 9-11 Commission noted the failure of the New York Fire Department's in-building radio coverage, as well as the lack of interoperability both within and between the various responding agencies. *The 9-11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, at 315-323 (July 22, 2004), *available at* http://www.gpoaccess.gov/911/Index.html. During Hurricane Katrina, operability was an even more acute problem than interoperability, as the complete devastation of the communications infrastructure left emergency responders without a core network on which to communicate. *The Federal Response to Hurricane Katrina: Lessons Learned*, Chapter 5, § 3 (Feb. 23, 2006), http://library.stmarytx.edu/acadlib/edocs/katrinawh.pdf.

A. **Public Safety Agencies' Use of Broadband Today**

Wireless broadband will play an important role in improving public safety communications interoperability and mission effectiveness. The emergency response community has voiced its need for advanced operable and interoperable data capabilities, in addition to its continued need for robust and reliable voice communications.[3] Difficulty with interoperability in existing voice operations for public safety can be tied to the development and evolution of those systems as implemented by thousands of separate jurisdictions and federal agencies. While much effort has gone into making those diverse operations interoperable, the development of broadband offers a significant opportunity to provide interoperability from the start.

The use of standards-based and vendor-neutral technologies will help spur deployment of both network connectivity and innovative new applications and services on more affordable devices. This approach will enable the delivery of wired and wireless technologies that will promote compatibility and interoperability across agencies, jurisdictions, and communities in a way that helps them leverage legacy systems as they migrate towards newer technologies. To that end, the Commission's National Broadband Plan (Plan) should consider the operational environment within the emergency response community, the community's current use of broadband applications, and how these two factors are influencing the community's approach to obtaining new broadband capabilities. The Plan must assess what is unique about the availability, reliability, security, and interoperability needs of the public safety and homeland security community at all levels of government. With an understanding of unique public safety requirements, the Commission will then be in a position to help chart out a course that leverages commercially-available networks and services to the maximum extent feasible. This is the path toward enabling public safety to have access to state-of-the-art, interoperable broadband data services and applications on a sustainable basis.

Taking into consideration their operational environment and their uses of broadband applications, public safety agencies can take three approaches to gaining access to broadband networks. Specifically, they may —

- Fund, deploy, and own a dedicated public safety broadband network that may be shared with other agencies;
- Partner with private sector broadband providers to deploy a network with shared costs; or
- Lease service from commercial service providers.

Most public safety agencies currently use separate networks for voice and data communications. This is primarily because current public safety voice networks can only support low data rate, narrowband capabilities, which limits opportunities for data applications. In addition, most commercial data networks do not currently meet latency requirements for

[3] *See, e.g.,* Comments of Public Safety Communications Officials-International, Inc. (APCO) (Nov. 12, 2009) ("APCO Comments") at 4-7; Comments of the Public Safety Spectrum Trust Corporation, PS Docket No. 06-229 (Oct. 16, 2009). *See generally* Comments of the National Telecommunications and Information Administration, PS Docket No. 06-229 (filed Nov. 9, 2009) ("NTIA 700 MHz Waiver Comments"), available at http://www.ntia.doc.gov/filings/2009/FCC_PS06229_700MHz_0911930130109.pdf.

mission-critical voice applications, cannot guarantee prioritization of public safety voice traffic, or do not offer push-to-talk (PTT) service.[4] Most public safety agencies have networks that meet their requirements for voice communications but these networks cannot support data capabilities; therefore, many agencies are planning to deploy secondary networks to provide data capabilities.

Public safety broadband applications today vary significantly. Most agencies use broadband for remote database access, remote reporting, and Internet/e-mail access, much of which is provided through leases with commercial service providers. Converged technology devices (such as smart phones) provide voice, data, and limited video coverage; however, their use is limited to administrative purposes because they do not meet all mission-specific requirements. The District of Columbia operates an experimental system with Federal agency participation.[5] During major events, such as the Presidential Inauguration, this system provides much-needed situational awareness.

The vast majority of Federal public safety agencies do not currently use broadband networks to support mission-critical voice communications. The Transportation Security Administration (TSA) of the Department of Homeland Security (DHS) is one exception. TSA uses commercial wireless broadband services in the 800 MHz spectrum for mission critical air-to-ground communications for Federal law enforcement officers in flight, as that is the only spectrum available for this application. This capability will soon include Voice over Internet Protocol (VoIP).

Immigration and Customs Enforcement (ICE), within DHS, is another exception. ICE uses commercial broadband networks for intranet access for laptops and other portable electronic devices, such as Blackberries, and for voice telephony applications. ICE requires exceptionally stringent security to safeguard law enforcement information and therefore allows broadband access only for authorized ICE end user equipment on which the required security controls have been installed and tested. ICE's law enforcement officers have mission-critical requirements for critical demand theater operations.[6] The lack of law enforcement priority on commercial broadband networks also necessarily limits ICE's usage of such systems. Despite such limitations, the Commission should consider whether use of commercial broadband networks, with adequate adaption by public safety agencies, may be a first step in the path to maximized broadband deployment.

---

[4] "Priority" in the public safety context refers to an assured connection for public safety or emergency response, including during particularly congested periods. A public safety network manager may be able to provide levels of priority based upon mission requirements and the needs of a particular emergency. When used in the context of IP-based broadband data networks, the term "priority" is functionally the same in that public safety seeks the ability to assure availability and quality of service under adverse, emergency conditions. However, the technical means by which these requirements will be met will be different, given the packet-routing, as opposed to circuit switched, nature of IP networks.

[5] U.S. Department of Commerce, NTIA, *Spectrum Policy for the 21st Century: A Public Safety Sharing Demonstration* (June 2007), http://www.ntia.doc.gov/reports/2007/NTIAWARNReport.htm. Department of the Interior Park Police are a prime partner in this program.

[6] They must have communications available on a 24x7 basis, with the majority of demand between 6 a.m. to 6 p.m., local time. Traffic includes voice, data, and multimedia, both originating and terminating on a variety of PTT devices and mobile computing devices/equipment. In addition, ICE management, supervisors, and administrative staff have mission requirements for medium and low demand theater operations to provide command and control, employee location tracking, communications assistance and lookup, and other support functions.

The vast majority of Federal public safety operations do not currently use specific broadband networks to support their operations. There is no specific Federal frequency allocation with sufficient bandwidth to support such a service. The Federal broadband applications in use are disparate, non-integrated systems transmitted over multiple modes of communication. In some cases, Federal agencies serve areas that also lack commercial alternatives. The Department of Interior (DOI), for example, has over 4,400 law enforcement and 7,000 fire fighting employees throughout the United States and its Possessions. Most of these employees are in remote locations with no access to broadband networks. In many areas that DOI serves, even commercial cellular voice service is unavailable. Where available, however, DOI public safety officials use broadband extensively for several purposes. While in fire camp, hundreds of wild land fire fighters may use broadband via satellite, existing infrastructure, or wireless local area networks for data on the blaze, including visual and infrared media imagery dissemination, resource ordering, Geographic Information System (GIS) data, and other activities.[7] However, commercial wireless carriers have deployed Fourth Generation (4G) advanced services in only approximately one percent of the rural areas that DOI services.

The U.S. Department of Agriculture's (USDA) Forest Service provides another example. It would utilize broadband primarily for wild land fire fighting, incident management, and to support approximately 650 law enforcement field personnel. However, access to broadband today is complicated by the fact that most of these law enforcement, fire and emergency response activities occur in very challenging and austere operational environments. The Forest Service's 10,480 fire fighters, and additional 5,000 "on-call" militia personnel, primarily operate in remote terrain often beyond the geographic footprint or line-of-sight of most commercial carriers. Even so, the Forest Service currently deploys personal computers into the field in those instances where landline or wireless connections are available, but they often operate at less than optimal speeds. If broadband Internet access were available, Forest Service personnel could make available topographical maps, weather information, personnel and vehicle asset tracking information, and logistics data for ordering and delivering equipment and supplies; send information on wild land fire incident status and personnel safety; and transmit public affairs updates.

As the frequency of wild land fires has increased, Forest Service first responders are relying on information technology to assist them in field operations at an accelerating pace. In such cases, little if any existing infrastructure is available to support these teams. Access to remote databases; fire decision support application tools; web-based applications; video teleconferencing; geospatial toolsets to monitor fire perimeters and survey incidents; and tools to support real-time communications with agency headquarters and other field command centers are critical to improving both the ability to respond effectively to such incidents as well as to enhancing the safety of those first responders.

Fire management personnel, often needed in remote regions, requires continuous transmission of operations-based communications on weather updates, vegetation information, logistics provisioning and on-line ordering, incident command directions, maps for ingress and escape paths and fire lines and safe zones. They may need wide area network capabilities for

[7] "Fire camp" refers to a temporary support facility providing food, sleeping areas, and medical and other resources for wild land fire fighters.

global Internet access or as a private network, using mobile SATCOM connections or standalone localized network access. In addition, Global Positioning System (GPS) connectivity is required to track people, firefighting vehicles and aircraft. These systems require end-to-end security systems and virtual private networks (VPNs).

B. **Public Safety's Needs for Wireless Broadband Networks and Applications**

1. Tactical Applications

Emergency responders envision using evolving enhanced broadband Internet access services and applications over the near and long term. Some potential applications of a tactical broadband network include:

- Real-time, full-motion streaming video for command post situational awareness;
- Digital imaging (for example, mug shots and building schematics) for law enforcement and first responders;
- Remote access to databases and report management systems to improve investigations (for example, the National Crime Information Center (NCIC));
- Remote access to biometric identification databases (such as U.S. VISIT) to improve effectiveness of patrol and enforcement operations;
- Mapping and GIS to improve response times and in support of border operations to provide officers and agents with in-field blue force and red force situational awareness;[8]
- Remote sensors (for example, biological and radiological) to detect life and movement;
- Mobile emergency management systems (EMS) applications for improved access to critical data;
- Weather and status broadcasts for fire-fighting purposes;
- Interagency, interoperable collaborative and distributed decision-making tools;
- Inventory management and accounting – web and other client-server applications (*e.g.*, fire resource ordering, law enforcement databases);
- GPS to track responders, fire fighting/law enforcement vehicles, and aircraft to enhance safety and tactical operations management; and
- Tactical voice over broadband (not offered commercially at this time but likely to be a future capability of interest) to supplant eventually Land Mobile Radio (LMR) networks.

2. Requirements

The Administration believes that capacity planning for public safety operations should be based both on geographic region and mission requirements. Requirements must also factor in surge capacity during joint operations and response events. The architecture and features of future broadband networks must enable seamless operation of disaster recovery capabilities throughout the Nation's emergency response community. Specifically, Federal agencies will require ubiquitous broadband coverage to support a variety of voice, video, and data requirements. In many instances, these mission-critical capabilities will be needed in regions that are unlikely to be served by commercial providers. It is not possible to determine fully

[8] "Blue" force generally refers to friendly forces while "red" refers to enemy personnel.

today how much spectrum will be needed for these applications on a going-forward basis, or if the current public safety spectrum allocation will ultimately be sufficient to meet future needs.

Existing legacy broadband wireless systems are not available in many remote areas.[9] Key border areas include long stretches in remote areas where there is no market to drive commercial investments in the communications infrastructure. This is also true in large forested areas where, for example, the Forest Service must routinely fight wild land fires with minimal infrastructure support. In these areas, Federal investment in infrastructure may be required to give Federal users—as well as public safety partners—access to broadband services that would not be available from commercial providers. In such cases, Federal and non-Federal public safety entities should coordinate to leverage all relevant public safety stakeholder resources. To accommodate the diversity within the stakeholder community, Quality of Service (QoS) requirements must be scalable to accommodate user and mission needs, but must also, at a minimum, satisfy law enforcement QoS and grade-of-service needs.

3. Role of Commercial Networks

a. Challenges

If commercial, wireless broadband networks are to serve public safety and homeland security communications needs, they ultimately must provide seamless interoperability, reliability, and robustness comparable to that of current public safety and homeland security systems. In keeping with current national plans, such networks must also be able to interoperate with National Guard and NORTHCOM Defense networks and operational capabilities.[10] Such networks must also provide sufficient capacity and access to ensure that public safety and homeland security minimum thresholds for degradation and blockage are not exceeded. In addition, the networks must accommodate priority service and offer accessibility and coverage to support emergency response operations.[11] Without prioritization, public safety services over commercial networks will be unreliable and overwhelmed by increased network congestion as the public responds to emergency events.[12]

The critical public safety question for the Commission to address in the Plan is how prioritization could best be developed and managed for homeland security and public safety purposes, consistent with private operators' commercial goals. In addition to priority, the public safety network needs to include a menu of connectivity, bandwidth, and transport options that provide the agility and diversity to assure as much access and capacity as possible despite congestion and network damage. The particular options available will shift over time as events unfold. Additional questions for the Commission are how to develop Project 25 (P-25),

[9] *See generally* "Wireless Broadband Access in Appalachia," http://www.arc.gov/index.do?nodeId=1813.
[10] "NORTHCOM" refers to the United States Northern Command, the Department of Defense (DOD) lead in national emergencies. DOD's ability to respond to local emergencies is restricted under the law. The Posse Comitatus Act, 18 U.S.C. § 1385, restricts the use of federal military for civilian law enforcement. In general, the National Guard is under the control of each state pursuant to Title 32 of the United States Code, until the President calls it into Federal service under Title 10.
[11] See *supra* note 4 for a definition of "priority service."
[12] APCO, for example, describes the inability of commercial networks, however cooperative, to support public safety access during the 2009 presidential inauguration and the over-congestion their networks experienced. APCO Comments, *supra* note 3, at 7.

broadband-capable, land mobile radios that can supplant high-cost voice-only networks and how to develop rugged devices that can stand up under harsh environmental conditions? [13]

The physical diversity, redundancy, reliability, and security of public safety services are characteristics that separate them from traditional commercial networks. For example, public safety networks have demanding requirements for hardening cell sites and other facilities to ensure network survivability. A public safety network must include redundancy and diversity elements to handle traffic during outages or emergencies. It must also be capable of interfacing with P-25 networks for interoperability, be compatible with existing Key Management Facilities (KMF) and be compatible with existing consoles for dispatch and command and control. Public safety network planners should study such requirements and, to the greatest extent possible, specify them in detail.[14] In addition, the network planning should explore how such requirements might be met through virtual networks embodying these characteristics, enhanced end user devices, or additional elements at the "edge" of the network, thereby allowing public safety to leverage core commercial broadband infrastructure to the maximum extent. Finally, the Commission should consider how resiliency and redundancy in a public safety network could be achieved through the proper application of competitive incentives for commercial carriers.

Backhaul requirements are dependent primarily on the density of public safety users and the ability to leverage existing infrastructure. Microwave, fiber optics or commercial Internet Protocol (IP) networks might supply that requirement. Typically, broadband infrastructure and backhaul must be fully redundant to support diverse routing in cases of outage or emergency. In rural or other areas where no current capability exists, however, even non-redundant operability would be an improvement over the status quo.

b. Virtual networks

The Commission should examine the feasibility of meeting public safety requirements through some use of commercial networks. In particular, the Commission should study how virtual public safety and homeland security networks can take advantage of commercial IP networks and new commercial 4G wireless networks. In this connection, and throughout its analysis of homeland security broadband needs, the Commission should consider all Federal communications and other spectrum-dependent systems, including the military and National Guard systems that could be called up in natural disasters, emergencies or hostile attacks.

It may be possible to address security and reliability concerns by using virtual networks that run on an IP backbone and hybrid commercial 4G wireless networks mixed with government-operated access in areas not serviced by commercial networks. A virtual private network can permit a secure link into a host commercial network or a "tunnel" tantamount to a hardwire connection. Such a network could be used, for example, to access databases for criminal information checks.

[13] P-25 is a suite of standards for digital land mobile radio communications that enables interoperable communications among Federal, state, local and tribal public safety responders.

[14] KMF refers to an application use to manage encryption keying and other functions for large groups of encrypted P-25 users.

The integration of a stand-alone public safety and homeland security network with a commercial transport layer may help isolate which network elements must be hardened. It may be that only key back office elements (such as Distributed Home Location Registers (DHLRs) and Roaming Tables[15]) and last mile segments of the public safety and homeland security network require increased security and reliability, while the commercial backhaul network's inherent reliability and security features are sufficient. The Administration recommends that the Commission study the feasibility, to the greatest extent possible, of using the core commercial infrastructure for public safety broadband deployment, and of meeting the unique needs of first responders through individuated end user devices or other communications elements near the network "edge."

Further, IP-based broadband networks offer survivability benefits.[16] However, if commercial IP-based networks are intended to be viable alternatives to public safety-grade emergency communications networks, then levels of network redundancy, diversity, and hardening must be agreed upon in advance through public/private partnerships.[17] In addition, distributed denial of service attacks could be a significant issue for IP-accessible communications nodes *(e.g.*, public safety answering points or emergency alerts) unless appropriate defenses are built into the network from the outset.

c. Air- and satellite-based data communications

In addition to addressing the emergency communications needs of different geographic areas, the Commission must understand that wireless communications support mission critical voice and data communications in the air. For example, TSA deploys Federal law enforcement officers on U.S. air carriers worldwide with a requirement for wireless, satellite-based broadband communications (outside the continental United States). This deployment is needed to support mission critical data and voice communications while onboard domestic carrier aircraft where other Federal law enforcement officers have law enforcement jurisdiction. The amount of spectrum usable for broadband in the 800 MHz commercial air-to-ground allocation is limited to 3 MHz.[18] There is the possibility of expanding coverage with satellite-based systems in the Ku-band, which is also offered commercially and is now available on two commercial airline carriers.[19]

---

[15] A "home location register" is a mobile subscriber database that among other things, authenticates users, and updates location data. "Roaming" refers to the use by one cellular operator's subscriber of another operator's network.

[16] These include common protocols allowing critical traffic to divert to alternative networks that are also IP-based. Survivability benefits also include self-healing abilities such as individuated routing of packetized data, so that loss of any discrete packet does not necessarily result in loss of the entire message.

[17] "Hardening" generally refers to a network infrastructure able to withstanding disasters, including by means of strengthened towers and additional backup generating capacity for cell sites.

[18] *See generally* FCC website, 800 MHz Air-Ground Radiotelephone Service, http://wireless.fcc.gov/auctions/default.htm?job=auction_summary&id=65.

[19] *See generally* "Row 44's in-flight Wi-Fi for commercial aircraft," http://www.ireport.com/docs/DOC-157799.

d. Recommendations

The Administration recommends that the Commission consider:

- Effectively and sustainably translating existing priority service programs to next-generation, IP-based networks, and, where appropriate, augment or replacing existing priority programs with other methods of achieving resiliency;[20]
- Leveraging the private sector's capabilities — including fixed, mobile, and hybrid-terrestrial satellites, and rapidly deployable networks, assets, and facilities — that can help ensure the success of public safety communications;
- Creating the appropriate incentives for the private sector to deploy the redundant and resilient capabilities that public safety requires;
- Examining the role of satellites in broadband deployment to rural areas and providing reliable nationwide communications where terrestrial services either do not exist or are temporarily out of service;[21]
- Encouraging providers to strengthen towers, improve electric power resiliency and standardize fuel requirements for backup power to withstand long-term outages of public power sources;[22]
- Piloting demonstration projects to validate IP-based networks' security and capability
- Clarifying prioritization requirements for emergency communications, national security and emergency preparedness resources;[23] and
- Addressing how public safety users should be authorized, authenticated, and provisioned with accounts when they access national commercial wireless broadband services.

4. Convergence of Voice and Data

Public safety agencies have a variety of requirements dependent on both the environment and the situation. In urban environments, public safety agencies need both on-street and in-building radio frequency (RF) coverage to support mission-critical voice and data communications. Those agencies may need to leverage legacy voice networks to provide more advanced communications, particularly in rural and remote environments where deployment is challenging. The Commission should consider whether such enhancements would be an effective first step to optimal broadband deployment in such regions. In all cases,

[20] *See generally* DHS website, "Wireless Priority Services," http://wps.ncs.gov/.

[21] Commercial satellite systems enable link diversity and independence from fixed infrastructure. For example, they form an essential part of National Guard emergency response communication systems.

[22] New or improved physical facilities may need to comply with Federal, state, and local regulations regarding the environment, zoning and land use, rights of way, pole attachments, tower marking and lighting, and safety and health considerations, and for the need for alternative, renewable power sources. Further, states regulate the capacity of fuel tanks for back-up generators.

[23] For example, during a pandemic, employees may be required to telework. Network congestion may occur as Federal employees try to access department/agency servers almost simultaneously. This is a practical justification for creation of virtual private networks. The Plan should consider the capability of networks to handle traffic surges in such anticipated situations and how priority access to broadband network resources for national security and emergency preparedness may be achieved. The Plan should define the criteria for priority access to such resources for national security emergency preparedness users.

communications must be robust against various sources of interference and noise to ensure intelligible communications.

As voice and data communications continue to converge, users have a greater expectation for both voice and mobile wireless data capabilities. Broadband systems that can provide reliable, interoperable voice and data communications will likely replace antiquated narrowband voice systems and low data rate networks. If mission critical voice applications are to migrate to broadband, systems will need to have sufficient control channel capability in high congestion areas, especially during special events and large gatherings, to support both a significant increase in text messaging and data traffic and call set up capability for national security and emergency preparedness (NS/EP) communications. Legacy voice networks must be effectively leveraged while the migration to broadband evolves.

Going forward, the Commission and relevant institutions in the public safety community must study how standards-based methods can deliver guarantees for NS/EP traffic that do not currently exist in broadband networks today. Moreover, any such prioritization would need to be sufficiently hardened to prevent its use as a method to execute a denial of service against the network.

5. Funding Models

There are a number of funding models for satisfying public safety's need for a nationwide interoperable broadband solution. These range from approaches that emphasize government or public safety entity provision of services to those that emphasize provision of services through commercial means. Such a network could be built off a "system of systems" concept or on the other end of the spectrum, a single nationwide commercial provider. Approaches that emphasize government funding are more likely to meet the public safety specifications but less likely to be built and a challenge to maintain. Those that lean on commercial providers may provide the greatest potential for rapid service deployment and standardization, but the least likely to meet strict public safety requirements and deployment in remote or rural areas.

The "system of systems" concept recognizes that a nationwide network may depend on smaller funding sources from local jurisdictions. It also emphasizes the value of those jurisdictions that have been the heart of traditional public safety, but jurisdictional boundaries have often been the source of interoperability issues. A national entity may be able to avoid these issues.

In between these extremes there could be other approaches including government licenses to commercial vendors who agree to meet public safety requirements or government systems that allow use for commercial purposes. Where the commercial vendors choose not to build out or where they do not meet public safety standards, public funding could fill these gaps. The Plan must determine which approach offers the greatest potential to satisfy all constituencies as well as the need for public safety broadband interoperability, robustness, reliability and prioritization.

The Administration encourages the Commission to permit demonstrations of innovative strategies for broadband implementation in the 700 MHz band, to the extent such strategies are consistent with the overall goals articulated here.[24] Demonstration projects should be built on top of the basic Internet standards that are certain to be at the heart of any public safety broadband wireless network services deployed around the country in the future.

C. **Mobile Wireless Broadband Networks Lessons Learned**

1. The Role of Partnerships

A key lesson learned regarding implementing and optimizing mobile wireless broadband networks is that partnerships across all levels of government are critical.[25] Such partnerships can support shared infrastructure projects, which are cost-effective techniques for pooling resources. Legal and regulatory barriers can hamper progress in this area, however, so these barriers must be resolved.

One partnership that offers great potential for encouraging broadband services in rural America is the Commission's ongoing cooperation with the USDA's Rural Utilities Service (RUS). The Commission should continue these outreach efforts with RUS and develop relationships with RUS stakeholders at the state, local, and tribal levels. The Commission can provide technical information and support to RUS staff. In 2003, the FCC established a similar partnership with the USDA with the creation of the Federal Rural Wireless Outreach Initiative. Pursuant to that initiative, the agencies agreed to begin reviewing their respective programs and regulatory structures so they could coordinate activities and therefore expedite the build-out of wireless communications throughout the nation. The coordination process involved discussions between the two agencies and included RUS's participation in the Commission's proceeding concerning how to increase rural investment and facilitate deployment of spectrum-based services in rural areas.[26]

Another successful partnership is TSA's use of wireless broadband services provided by a commercial vendor for air-to-ground communications. The system has been developed through a public-private partnership and was made possible by the October 2006 FCC auction of 4 MHz of spectrum in the 800 MHz range for commercial air-to-ground communications. The public-private partnership was coordinated by the inter-agency Air-to-Ground Communications

---

[24] *Service Rules for the 698-746, 747-762 and 777-792 MHz Bands; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, Second Further Notice of Proposed Rulemaking, 23 FCC Rcd 8047 (2008) and Third Further Notice of Proposed Rulemaking, 23 FCC Rcd 14301(2008).

[25] *See generally* DHS, "National Emergency Communications Plan," at 6, 15, 37, 64, 65 (July 2008), http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf.

[26] The RUS's participation in Indian Telecommunications Initiatives' Regional Workshop and Roundtable events demonstrates how leveraging the RUS can help engage traditionally underserved communities. During these events, RUS participated in panel discussions about various loan and grant programs available through its office. This joint Federal partnership, which helps link Commission programs with RUS financial resources, is an important way to promote broadband deployment on Tribal lands, where it can bring important economic development, educational, and health care opportunities to traditionally underserved rural communities. The FCC and RUS have engaged in similar outreach efforts with stakeholders at the state level, such as Tennessee and Kansas, where they explained how Federal programs can be used to improve broadband deployment in rural communities.

Working Group chaired by TSA.[27] As a result of this partnership, the post-auction owners of the spectrum more clearly understood the public sector's requirements for using the spectrum to support mission critical data and voice communications.

2. Taking Advantage of Federal Procurement Vehicles

Many federal agencies can contribute to the goal of improving public safety communications capabilities nationwide. The General Services Administration (GSA) is a crucial partner for the implementation of standardized and interoperable systems. GSA's Federal Acquisition Service (FAS) is positioned to use all available procurement vehicles as appropriate to assist in the deployment and implementation of the National Broadband Plan. FAS procurement vehicles can help ensure consistent deployment of standards-based communications and information technology (IT) capabilities for emergency responders, providing the foundation for interoperability for Federal, state, local and tribal emergency responders.[28] The Commission should collaborate with GSA throughout the implementation of the National Broadband Plan to promote the use of these procurement vehicles to ensure these benefits are realized and complement the public safety goals for broadband deployment. The Commission should also explore other ways to assure that all public safety agencies leverage existing work on standards and other relevant studies and research in a coordinated manner.

3. Leveraging Commercial End-User Devices

When compared to a coverage-engineered interoperable wireless network, today's deployed base of cellular phones and broadband networks offers only limited usability to the law enforcement community. Although it may be acceptable to use cellular phones as a backup or for covert reasons in some limited circumstances, these phones lack certain features of a tactical wireless network that are mission-critical to all Federal law enforcement operations, specifically:

- High-speed PTT;
- Direct mode (radio-to-radio communications without network infrastructure);
- End-to-end Advanced Encryption Standard (AES) encryption;
- Over-the-Air Rekeying (OTAR); and
- Signal coverage.

The Commission should consider whether it would be possible to develop standards and requirements for public safety end user devices that would leverage existing commercial handsets to the maximum extent, capitalizing to the greatest degree on economies of scale. At the same time, the Commission should consider whether such handsets and other elements near the network edge can be adapted to use a commercial core network or be capable of direct access to commercial 4G wireless networks. This might allow public safety to target broadband investments to mission-essential network components.

[27] The Federal Bureau of Investigation, National Aeronautics and Space Administration, Federal Aviation Administration, DOD, the Commission, domestic air carriers, and flight and cabin crew unions participated in this group.

[28] New York City, Washington, D.C., Baltimore, and Corpus Christi are cities with broadband data networks that have public safety applications. The Washington, D.C., pilot is known as the "Wireless Accelerated Responder Network" (WARN). *See generally supra* note 5 and accompanying text.

D. **The Role of Commercial Broadband Service Providers**

The private sector plays an important role in emergency response, and its capabilities can enhance the resilience and reliability of public safety communications. Based on the currently deployed capabilities of commercial networks, public safety's ability to rely on these systems is very mission dependent.

At the same time, some agencies have successfully leveraged commercial networks. For example, some elements of DHS' Federal Protective Service (FPS) use commercial handheld or hand-transportable mobile data/multimedia display devices and applications supported with mobile data/multimedia communications. These devices and applications can:

- Provide Automatic Vehicle Location (AVL), vessel tracking, and flight following for asset position-location situational awareness, which supports coordination of operational activities, identification of available assets, and optimal direction of mutual aid;
- Provide immediate tactical access to key case, biometric identification or mission data and report generation, minimizing the need for personnel to return to the office to complete paperwork—maximizing their time in the field and the casework they can perform while in the field;
- Enable personnel to obtain more tactical database information than when such requests must be processed by communications assistants/dispatchers over radio voice calls, manual terminal access and lookup, and return radio calls; and
- Eliminate time-consuming database lookups from communications assistant/dispatcher operations, thus freeing voice channel time for true emergency calls or surveillance/arrest coordination missions.

Notwithstanding these valuable capabilities, as previously noted, the system would benefit from direct mode (radio-to-radio without infrastructure), end-to-end AES encryption, OTAR, and expanded signal coverage.

Given the enormity of the investment needed for nationwide public safety broadband coverage, commercial network sharing and gap filling should be part of the solution as long as commercial systems can provide the reliability, availability (including priority) and security mandated by public safety/homeland security users, or allow public safety to meet these needs through non-core network elements near the network "edge." Moreover, commercial systems can drive technology solutions, such as handset components, in a more cost effective manner. Federal users should also expect to build and operate systems in partnership with public safety and homeland security practitioners at all levels of government.

E. **Expected Bandwidth Use for Public Safety**

Today's public safety networks support transmission speeds between 9.6 kilobits per second (kbps) and 19.2 kbps. This range cannot support applications beyond standard text communications. Additionally, some public safety agencies believe that commercial Third Generation (3G) wireless networks cannot adequately support requirements for higher bandwidth applications such as streaming video. While specific projected bandwidth requirements cannot

be stated without extensive analysis, it is likely that bandwidth requirements would begin at 128 kbps and increase for graphics intense applications up to 4-10 megabits per second.

Current spectrum allocations in the VHF, UHF and other bands do not provide sufficient broadband capacity to meet evolving requirements for converged voice and data. The Commission should assess whether the 12 MHz of spectrum currently allocated to public safety in the 700 MHz band will be sufficient to meet the needs of all public safety users for converged voice, video and data traffic, given that individual regions will have different requirements. As part of that assessment, the Commission should consider how that public safety allocation could be supplemented via commercial or other arrangements.

To provide precision and additional clarity into public safety needs, the Commission should conduct a quantitative analysis of the minimum preferred thresholds for emergency responders' use of bandwidth-intensive mobile video, data, and other public safety applications to support operability, interoperability, and continuity of communications. After defining quantitative threshold data, the public safety community can coordinate with commercial service providers to validate and endorse the minimum thresholds needed to support anticipated uses. Public safety's use of broadband technologies, services, and applications are still in the early stages of development; as a result, sound bandwidth usage requirements are not yet well understood or defined. Further coordination will be needed to adjust periodically the minimum thresholds as new technologies and services emerge and bandwidth needs evolve.

Mobile broadband offers performance benefits for minimal added cost, but any use of mobile data/multimedia must be properly designed, certified and accredited, and implemented to optimize mission performance and thus compatibility with existing data sources. A formal phased—or evolutionary—approach for fast-prototype development should take into account both the relevant data Enterprise Architecture and a systems engineering framework.

F. **Ensuring Interoperability Among Public Safety Broadband Systems**

Wireless broadband services will play an important role in improving public safety and homeland security communications interoperability and mission effectiveness. To facilitate broadband's ability to advance these interests, the National Broadband Plan should define a minimum set of requirements that will establish a baseline of interoperability between networks and allow wireless users to roam. These standards should permit seamless day-to-day public safety operations, as well as emergency deployment in aid of sister jurisdictions. A standard that would enable a single device to roam across a nationwide footprint would ensure economies of scale, promote an open standard fostering competition from vendors, and reduce long term operations and maintenance costs.

Another pivotal issue is the eligibility of Federal agencies to access any nationwide public safety broadband network for public safety communications uses.[29] Federal agencies have aligned with their state, local, and tribal partners in mutual aid agreements, shared spectrum and tower facilities, and shared infrastructure/system arrangements. Through enhanced planning efforts, Federal, state, local, and tribal public safety agencies often have been able to operate on

[29] *See generally* NTIA 700 MHz Waiver Comments, *supra* note 3.

the same statewide or regional communications system, thereby achieving seamless interoperability, cost and spectrum efficiencies, and enhanced operability. In some cases, Federal agencies' public safety or homeland security missions may require daily operational access. In others, Federal agencies may intervene in disaster recovery or other emergency response efforts. In either case, the Administration believes that Federal agencies should be treated the same as their local, state and tribal partners with respect to access, reciprocity and any user fees.

The Administration believes that maximizing the benefits of nationwide public safety broadband interoperability will require access not only by first responders, but by emergency response support agencies, including critical infrastructure providers. Critical infrastructure includes the nation's transportation network (including highways, transit, waterways, and ports), the electrical grid, and other public utilities such as pipelines and water supplies. Different emergencies present different threats. Some involve transportation services or other critical infrastructure.[30] These emergency support agencies are critical to public safety during daily incidents, but even more so during local, regional or national disasters. Meaningful planning for a public safety broadband network should take such critical users into account.

Transportation agencies, through their operations centers, can share important data with their public safety partners. For example, information on road closures, detours, and video of the incident scene would help evacuation of victims and access by emergency response vehicles. Transportation assets can also be brought to bear more quickly if heavy equipment or other unique services are needed.

Regardless of the regulatory regime the Commission ultimately develops, it should consider whether a public safety broadband network operator, or incident commander, needs to be able to prioritize network use among all critical users, including critical infrastructure providers. Planning for a public safety broadband network should take into account non-traditional public safety groups in transportation and other critical infrastructure disciplines.

[30] Ten years ago, a gasoline pipeline ruptured in Bellingham, Washington, polluting a nearby waterway and killing three individuals in a subsequent fire. In 2005, terrorists bombed London subways, killing 79 and injuring 700. Earlier this year, a commercial airliner crash-landed in the Hudson River in New York City. In each case, transportation or infrastructure professionals were key responders, bringing expertise and resources beyond those held by traditional first responders.

G. **Convergence of Mobile Broadband Data and Voice Networks**

Two key issues associated with convergence are interoperability and security. With respect to interoperability, the Commission should consider ways to adopt a wireless broadband architecture framework necessary to achieve seamless, coordinated, and integrated public safety and homeland security communications operability and interoperability that would enable different agencies at all levels of government to communicate with one another and to exchange critical information during emergencies and routine operations. For a national emergency, the full spectrum of Federal (civil and military), State, and local capabilities must be interoperable. The efforts of the National Communications System should be included in any planning.[31] A common framework would also prevent the creation of non-interoperable stove-piped systems.

DHS has begun to develop a technology roadmap to advance efforts on interoperable communications. In addition, DHS's Office of Emergency Communications (OEC) is updating the National Emergency Communications Plan (NECP) to focus on improving current voice technology while building a broader emergency communications and next generation technology vision. The vision is defined along two paths—a Mission Critical Voice Path and an Integrated Emergency Communications Path. Moreover, any Federal solutions operating on a nationwide public safety network must be based on open standards and be vendor-neutral. Roaming agreements between public safety and Federal systems are needed to provide seamless broadband coverage and sufficient access.

With respect to security, convergence of these networks will present another challenge. Federal, state and local public safety organizations will use a nationwide broadband network for a wide variety of applications to meet mission specific requirements. In some cases, the network will replace or augment existing technologies, such as mission critical voice communications. In those situations, users will expect the new network to provide the same security features as those provided by legacy systems. In other cases, the network will be used in novel ways and users may not have the same security expectations, particularly if faced with trade-offs between security and cutting-edge capabilities. Therefore, the Plan should consider the development, implementation and management of preemptive access capability that would enable prioritization and interruption capability for homeland security applications. Without prioritization management, public safety services over commercial networks will likely be unreliable and could be overwhelmed by increased network congestion as the public responds to events. The Commission should explore whether commercial networks can provide core infrastructure for public safety applications or virtual networks with such capabilities.

To meet the requirements of Federal, state and local public safety organizations, the network must be able to support flexible security architecture. For example, in accordance with DHS Management Directive 4300, DHS requires all of its communications equipment to be AES encrypted and certified before field implementation. DHS also requires this level of security as it

[31] The National Communications System is an interagency group of 24 Federal departments and agencies which assist the President, the National Security Council, the Homeland Security Council, the Office of Science and Technology Policy, and the Office of Management and Budget, in the coordination and planning for national security and emergency preparedness communications for the Federal Government under all emergency circumstances, including crisis, attack, recovery, and reconciliation.

moves into a broadband environment. Hardening of certain network elements, such as home location registers, roaming tables and other critical databases may be necessary to ensure resilient communications during a crisis and prevent intentional disruption of emergency response services. Similarly, sufficient capacity, or prioritization capabilities, will need to be available to ensure that national security and emergency preparedness communications continue to function properly during major events (parades, concerts, emergencies, etc.) when the volume of data and voice communications may exceed normal network capacity. At the same time, any deployed prioritization capability will also need to be hardened to prevent its use for executing a denial of service attack against the network. The Commission should study whether such requirements can be met through targeted additional investments to a foundational core commercial network.

H. **Conclusion**

Making an interoperable public safety broadband network a reality requires both practical sense as well as a vision for the future. Near term, the Commission, the Executive Branch agencies and their local, state and tribal counterparts, must try to meet public safety's immediate broadband needs in ways that leverage available resources. This entails exploiting existing core infrastructure while equipping end-user devices and other aspects of the network edge for public safety's unique needs. It also requires creating the appropriate competitive incentives for commercial operators to deploy the redundant and resilient infrastructure that public safety requires. Throughout, the Commission must pursue the ultimate goal of an interoperable public safety broadband network that meets public safety's specifications and is available throughout all regions of the country, however remote.

III. **NEXT GENERATION 911 (NG911)**

A. **The NG911 Elements of the National Broadband Plan**

Trends in personal communication technologies are accelerating the obsolescence of the current 911 system. The current circuit-switched infrastructure of the 911 network cannot receive digital data (*e.g.*, text messages, photographs, and video) from the communication devices commonly used by the public. Because these outmoded networks cannot provide the public with access to 911 services from newer technologies and devices, 911 networks and call centers will need to change.

The goal of NG911 is to enable the general public to make a 911 "call" (that is, any real-time communication–voice, text, or video) from any wired, wireless, or IP-based device, and allow the emergency services community to leverage advanced call-delivery and other functions through new internetworking technologies based on open standards.

In the NET 911 Improvement Act of 2008, Congress tasked the National E911 Implementation Coordination Office (ICO) to develop "a national plan for migrating to a national IP-enabled emergency network capable of receiving and responding to all citizen-activated emergency communications and improving information sharing among all emergency

response entities."[32] This Migration Plan identifies and analyzes 911 system migration issues and assesses potential options to resolve them consistent with the requirements of the NET 911 Improvement Act.[33] This plan describes migration scenarios, identifies benefits and barriers and other implementation issues, and provides results from recent trial deployments and cost-value-risk analyses. It highlights the key milestones that must be achieved and identifies legislative issues that must be considered if widespread IP-enabled 911 is to become a reality. The Migration Plan also examines location technologies and associated advantages and disadvantages for NG911 deployment.

B. **Broadband Infrastructure Requirements**

Some of the infrastructure requirements for NG 911will depend on the infrastructure that service providers are able to provide, both today and in the near-term. The functions that 911 centers make available to their callers will likely expand based on the available bandwidth, instead of technical requirements driving improvements in throughput.[34] Additionally, disparity between communities with and without broadband (or without "sufficient" broadband) may result in multiple requirements baselines, dependent on the underlying infrastructure, rather than a universal set of features.

Regardless of today's limitations, the public sector will continue to pursue innovative ways of utilizing the features and functions of commercial broadband networks and devices to access emergency communication systems. The broadband infrastructure requirements will include the capability to transmit and receive multimedia including voice, video, images, text, and data and will be dependent upon the ability to transfer calls between Public Safety Answering Points (PSAPs) along with all collected data. Identifying specific infrastructure requirements today is difficult, as the functional requirements are still under development. However, as PSAPs move toward NG911 technologies and accept rich forms of media, a corresponding improvement in their infrastructure (and the infrastructure of their service providers) will be necessary.

C. **NG911 Technical Standards**

As with NG911 requirements, NG911 standards also have not been comprehensively defined and much work remains before broadband standards are completed. The Department of Transportation's (DOT) Office of Emergency Medical Services (OEMS) has taken steps to compile (in conjunction with 911 stakeholders) a list of current technical standards activities related to NG911. Once this list is compiled and 911 stakeholders have provided input, the OEMS will conduct a gap analysis to identify those functional requirements of NG911 for which technical standards are not being developed. OEMS will utilize the list and the gap analysis to form and post a comprehensive list of NG911 technical standards, and post, monitor, support and promote the activities of Standards Development Organizations (SDOs) in completing NG911 technical standards. OEMS will also afford all SDOs access to the 911 Technical Assistance

---

[32] Pub. L. No. 110-283, § 102, 122 Stat. 2620, 2623 (codified in 47 U.S.C. § 942(d)).

[33] National E911 Implementation Coordination Office, *A National Plan for Migrating to IP-Enabled 9-1-1 Systems* (Sept. 2009), http://www.e-911ico.gov/NationalNG911MigrationPlan_sept2009.pdf.

[34] *See generally* Intelligent Transportation Systems, U.S. Department of Transportation website, http://www.its.dot.gov/ng911/pdf/NG911_HI_RES_Requirements_v2_20071010.pdf.

Center (TAC) and 911 Information Clearinghouse that will become operational in late calendar year 2009. They will provide subject matter experts, documents, articles and other technical, operational and policy information related to 911 and emergency communication. Results of DOT's NG911 Initiative continue to help shape the important work of the SDOs.

D. **Deployment of NG911 Technologies and Services**

The DOT's NG911 Initiative demonstrated key functional requirements as part of the project's Proof-of-Concept (POC) phase. This demonstration of technology provided the 911 community with a preview of emerging NG911 technology and offered the vendor community an early opportunity to demonstrate their products. The POC findings have assisted in the development of new products and helped guide the community on how best to develop, test, and implement NG911 solutions.[35]

The availability of grant money for IP-based networks will encourage their deployment. DOT's National Highway Traffic Safety Administration (NHTSA), in coordination and cooperation with NTIA, is currently administering a $43.5 Million E911 grant program, which was authorized under the ENHANCE 911 Act of 2004.[36] The Act authorizes grants for the implementation and operation of Phase II enhanced 911 services and for migration to an IP-enabled emergency network. The grants were awarded to 30 states and territories on September 25, 2009 and are currently being tracked and managed by NHTSA. These grants have enabled states and territories to plan, develop and implement both phase II wireless 911 or IP-based emergency communications network.

E. **Regulatory Roadblocks for NG911 Deployment**

Many current state laws and administrative rules are outdated and do not adequately reflect the governance and policies of modern NG911 systems. DOT's *NG911 Transition Plan* outlines strategic options that are available at all levels of government to address governance and policy that could affect migration to NG911.[37] These options include potential strategies or paths that would:

- Clarify jurisdictional frameworks and responsibilities and identify the coordination required at each level of government to enable NG911;
- Update legislation, regulations and policies to reflect modern communications and NG911 system capabilities; and
- Ensure continued access to the 911 system using current and future devices and services with which users would reasonably expect to access to 911.

Further, the Migration Plan outlines key actions necessary for stakeholders throughout the 911 community, such as the Commission, to implement NG911. Included in this report are

[35] U.S. DOT Next Generation 9-1-1 Initiative, Proof of Concept Testing Report, September 2008, http://www.its.dot.gov/ng911/ng911_pubs.htm.
[36] Pub. L. No. 108-494, § 104, 118 Stat. 3986, 3987-3988, (*codified at* 47 U.S.C. § 942(b) (2006)).
[37] U.S. DOT Next Generation 9-1-1 Initiative, Transition Plan, February 2009, http://www.its.dot.gov/ng911/ng911_pubs.htm.

recommendations on legislative changes, including definitions, which are necessary to facilitate a national IP-enabled emergency network. The recommendations also include:

- The need for 911 laws and regulations to be updated to assure they are technology-neutral; and
- The critical need for establishing responsibilities for generating and delivering accurate, real-time location information.

F. **Technologies for Automatic Location Identification**

As required by the NET 911 Improvement Act, the ICO identified and analyzed location determination technologies and solutions for nomadic devices, office buildings, multi-dwelling units and to serve those individuals with disabilities. Appendix B of the Migration Plan describes the growing number of location determination technologies that are available. However, the roles and responsibilities for generating and delivering the location information is a major issue yet to be resolved.

New and emerging location approaches are now available or currently under development to serve non-emergency needs such as social networking and product inventory control for indoor and outdoor applications. Whether any of these will be suitable for response-quality 911 location has not yet been tested. More research into these applications and options is needed.

Location technology affects 911 calls at two points: first, to route the call to the appropriate PSAP and second, to provide information to locate the caller. While location information currently delivered may be adequate for routing 911 calls, there is presently no single or hybrid technology that can provide location information from mobile IP devices on converged networks that is adequately accurate for first responders to locate callers.

To be most useful to the PSAP, the location of the caller needs to be provided upon call delivery. Although landline phones provide location information at the time the 911 call taker receives the call, there is a delay for providing similar information for wireless callers. NG911 requirements seek to eliminate that delay for all callers, regardless of device or technology used to connect to the PSAP.

G. **Enabling Emerging Internet Applications**

Implementing NG911 solutions will take a coordinated and concerted effort of many stakeholders across the 911 community. Individuals and groups from outside the traditional 911 community will also share the responsibility of enabling NG911 technologies. The DOT's NG911 Initiative has initiated documentation of the process, strategies, and risks and associated mitigating actions for the transition from today's 911 to NG911. Two documents are particularly useful to stakeholders:

- NG 911 Initiative: *NG9-1-1 Transition Plan*
- NG 911 Initiative: *NG9-1-1 Procurement Tool Kit*

These plans outline the many aspects of the NG911 Transition, including issues relating to planning, policy and governance, security, standards and technology, and training. The *NG911 Transition Plan* offers a high-level description of the issues and potential solutions regarding stakeholder involvement. It also documents the available options and strategies for addressing transition issues for 911 Authorities choosing either a coordinated or unilateral approach and within this context, creating a tailored approach to resolving issues as they arise.[38]

The *Procurement Tool Kit* makes it easier to assess the information NG911 stakeholders need to plan for procurement and implementation, and to gauge the overall success of their efforts.[39] It describes the essential steps in planning for NG911 and outlines the resources available to assist 911 organizations and other stakeholders. This tool kit provides a self-assessment tool, planning tools, recommended options, and methods to identify issues that may confront 911 authorities interested in implementing IP-based 911 emergency communications systems. In addition, it discusses what changes and procurements are possible and provides a path forward for state and local authorities.

H. **Conclusions and Recommendations**

Much work remains before NG911 is realized; despite the barriers, NG911 is achievable. The Migration Plan outlined the obstacles and mechanisms to overcome them, and the benefits of moving towards the next generation of 911 services. There are a large number of operational, economical, and institutional issues that must be addressed and reconciled to successfully implement the NG911 system across the Nation. Implementing NG911 will likely be a complicated process, requiring the effective, timely and willing cooperation of an array of stakeholders, including the Commission. Although the rationale for deploying NG911 is compelling, the extent to which all 911 stakeholders move toward IP-enabled 911 will be affected by how they resolve or mitigate the institutional issues.

In crafting a National Broadband Plan, the Commission should recognize and build on both the DOT's NG911 Initiative and the ICO's IP Migration Plan. Additionally, the Commission should convene forums with public safety organizations, service providers, and advocacy groups to identify obstacles and mechanisms needed to implement NG911 regulations. It should call on its Communications Security, Reliability, and Interoperability Council (CSRIC) to consider issues related to NG911 implementation as necessary and make appropriate recommendations to the Commission.[40] Further, the Commission should work with appropriate Federal agencies to educate the stakeholder community (for example, EMS, 911, fire and law enforcement) on the effectiveness and understanding of all aspects of NG911. Finally, consistent with the *NET 911 Improvement Act*, the Commission should work cooperatively with public safety organizations, industry participants, and others to develop industry best practices to promote consistent standards in connection with IP-enabled E911 or NG911 services.[41]

---

[38] U.S. DOT Next Generation 9-1-1 Initiative, Proof of Concept Testing Report, September 2008, http://www.its.dot.gov/ng911/ng911_pubs.htm.
[39] U.S. DOT Next Generation 9-1-1 Initiative, Procurement Tool Kit, September 2009, http://www.its.dot.gov/ng911/ng911_pubs.htm.
[40] *See* http://www.fcc.gov/pshs/advisory/csric
[41] Pub. L. No. 110-283, § 101, 122 Stat. 2622-2623 (codified in 47 U.S.C. § 615a-1(h)).

IV. CYBERSECURITY ELEMENTS OF THE NATIONAL BROADBAND PLAN

> *Cyberspace touches practically everything and everyone. It provides a platform for innovation and prosperity and the means to improve general welfare around the globe. But with the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations, private enterprises, and individual rights. The government has a responsibility to address these strategic vulnerabilities to ensure that the United States and its citizens, together with the larger community of nations, can realize the full potential of the information technology revolution.*[42]

President Obama's recent call to action on cybersecurity is motivated by the fact the Internet has become "woven into every aspect of our lives. It's the broadband networks beneath us and the wireless signals around us, the local networks in our schools and hospitals and businesses, and the massive grids that power our nation. It's the classified military and intelligence networks that keep us safe, and the World Wide Web that has made us more interconnected than at any time in human history."[43] The Nation relies increasingly on cyberspace as a vehicle for innovation, economic competitiveness, national prosperity, and a tool for efficiency, transparency and accountability in government.

Along with the clear benefits and growing utility afforded by cyberspace, come a range of emerging risks and growing threats by a host of adversaries, including organized and individual criminals, nation-states, and terrorists. These adversaries act for a wide variety of purposes, including for financial gain or strategic advantage obtained by stealing or destroying sensitive information. Cyber attacks continue to be mounted against government, military, commercial, and private networks, and national critical infrastructure networks (*e.g.*, energy, water, sewage, transportation, banking and financial networks.)

The geographic extent and decentralized nature of cyberspace complicates the task of protecting providers and users from malicious attacks. When the telecommunications industry was characterized by centrally-controlled telephone and data networks of limited reach, a small number of network operators could work with law enforcement agencies to develop a clear set of security strategies. In contrast, the global scale and the welter of interconnected networks, applications, and services that characterize cyberspace require new cybersecurity strategies and more innovative cybersecurity processes in both the government and the private sector.

A. Cybersecurity Challenges Require Unique, Internet-aware Solutions

Successful strategies for managing cybersecurity threats will begin by recognizing and leveraging the characteristics of the Internet. The layered model, described in the introduction (See Figure 1), illustrates the allocation of cybersecurity responsibilities in each layer. At the top, with respect to the Applications, Services, and Equipment layer, the private sector must lead

---

[42] *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, at I (May 2009) (*Cyberspace Policy Review*), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[43] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," May 29, 2009. *See* http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

in developing innovative security protection technologies and practices. The government is responsible for catalyzing national strategies to secure cyberspace. Here, as in society generally, the key government roles are to assure vigorous domestic law enforcement and appropriate national security defensive and offensive postures. The legal system should protect consumers and personal privacy, and safeguard civil liberties, as well as provide for appropriately robust law enforcement, intelligence, and other cyber-related enforcement. By clearly defining providers' obligations and providing a swift mechanism for addressing violations, the legal system can encourage innovative security practices, and assure adequate public and private sector investment in security technology.

Technical Standards and Protocols development activities guide the operation and evolution of the Internet and enable the wide range of application and services, a vital source of value of the Internet to individuals and society. Enhancing security in technical standards and protocol development activities, both through better technical architecture and management best practices, can propagate security advances throughout the cyber-infrastructure with far more efficiency than traditional regulatory action or uncoordinated market signals. Great leverage can be gained from concerted public-private partnerships in this area. In most cases, private sector-led standards-setting is still appropriate, but active participation by appropriate Federal agencies – the National Institute of Standards and Technology (NIST) and DHS – will be vital in order to contribute requirements and recommend priorities. Based on this input, the private sector should then be given an opportunity and incentive to develop technical and management solutions in an open, transparent manner.

The Telecommunications Networks Core is an area that has a long history of collaboration among the Nation's communications infrastructure providers. The National Coordinating Center for Telecommunications (NCC) assists in the initiation, coordination, restoration and reconstitution of national security/emergency preparedness (NS/EP) telecommunications services or facilities. Through the NCC, the Federal Government and telecommunications companies address NS/EP telecommunications service requirements, including both real-time responses to natural and man-made disasters and long-term efforts to plan, develop, and support a more resilient national and international communications system. The NCC enables the rapid exchange of information and expedites NS/EP communications responses. Although the NCC focuses primarily on the NS/EP telecommunications service requirements of the Federal Government, the NCC also monitors the status of all essential telecommunications facilities, including public switched networks.[44]

Public and private sector interests, involved in applications, technical standards, and/or network operations, have a shared responsibility to create effective, coordinated, and cooperative cybersecurity strategies that focus on deterrence, detection, and mitigation of cyber threats. In a proclamation issued in October, marking the start of National Cybersecurity Awareness Month, President Obama highlighted "the responsibility of individuals, businesses, and governments to

[44] DHS has recently collocated NCC and the United States Computer Emergency Readiness Team (US-CERT) operational resources as well as the National Cyber Security Center, in the National Cybersecurity and Communications Integration Center (NCCIC). This is a joint watch floor operation capable of managing both cyber and communications incidents of national scope.

work together to improve their own cybersecurity and that of our Nation."[45] Providers of broadband communications services, including broadband Internet access and "interconnected" voice over IP (VoIP) services, must assist law enforcement in maintaining the necessary tools to disrupt and apprehend criminals who use their facilities and services.[46] Applications providers and network operators need to promote deterrence measures by developing innovative features and/or operational procedures that further enhance the security of their products and services. As an operator of large government networks and in its capacity to detect and neutralize cyber threats, the Federal government has a wealth of experience and substantial knowledge of cyber threats facing the Nation. This critical information can prove most useful to commercial providers as they design more secure products and services, and to the technical community in developing ever more effective security protocols. The following section describes Federal agency activities to identify and mitigate cyber threats, and collaborative efforts to share critical information with industry and the security research community.

B. **Federal Government Activities Relating to Cybersecurity**

The Administration is developing a strong leadership component to organize Federal cybersecurity efforts. Based on a key recommendation from a 60-day comprehensive review of federal cybersecurity activities, the President is creating a new office in the White House to be led by a Cybersecurity Coordinator, who will coordinate such activities and work with National Security Council and National Economic Council staff.[47] The Cyberspace Policy Review also articulates other recommendations being implemented by Federal agencies.[48] Those recommendations include initiating a national public dialogue and awareness campaign on cybersecurity, evolving effective public-private partnerships to secure cyberspace, and working with international partners to enhance cybersecurity.

Many Federal agencies are involved in a wide range of domestic and international cybersecurity operations that are responsive to those recommendations. They support educational and training opportunities for cybersecurity professionals as well. Some of these activities are described below, along with measures designed to promote more secure Federal networks.

---

[45] "National Cybersecurity Awareness Month, 2009, A Proclamation by the President of the United States of America" (Oct. 1, 2009), http://www.whitehouse.gov/the_press_office/Presidential-Proclamation-National-Cybersecurity-Awareness-Month.

[46] *See* Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. §§ 1001, *et. seq*. (2006); *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, First Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd 14989 (2005), *aff'd sub nom. American Council on Educ. v. FCC*, 451 F.3d 226 (D.C. Cir. 2006). "Interconnected" VoIP services permit users to receive calls from and terminate calls to the public switched telephone network. By its terms, CALEA does not apply to providers of information services, a category that likely includes most Internet-based services and applications. *See* 47 U.S.C. § 1001(8)(C)(i) (2006).

[47] Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

[48] *Cyberspace Policy Review*, *supra* note 42, at iv-v.

1. Domestic Operations

DHS leads the Federal Government's efforts to protect civilian federal systems.[49] DHS's National Cyber Security Division (NCSD) maintains relationships with government agency partners to fulfill its cybersecurity mission.[50] NCSD's United States Computer Emergency Readiness Team (US-CERT) coordinates efforts to improve the Nation's cybersecurity posture, promote cyber information sharing, and manage cyber risks to the Nation. US-CERT focuses on improving customer service and interagency coordination in a variety of ways. For example, the Joint Awareness Cyber Knowledge Exchange, which meets monthly, provides a classified forum for Federal Departments and Agencies to exchange cyber threat and defense information, with US-CERT providing regular briefings and updates about ongoing threats and incidents.

Other NCSD programs also offer significant opportunities to improve agency coordination, and NCSD continues to look for new and better ways to build partnerships. Through the Trusted Internet Connection (TIC) Initiative and deployment of the National Cybersecurity Protection System (NCPS)—operationally known as EINSTEIN—NCSD can coordinate with all Federal civilian Departments and Agencies to reduce and consolidate external connections (access points) and enhance security postures.

NCSD collaborates closely on cybersecurity matters through the Critical Infrastructure Partnership Advisory Council (CIPAC) under the National Infrastructure Protection Plan (NIPP) framework. Since 2007, under CIPAC, NCSD has co-chaired the Cross-Sector Cyber Security Working Group (CSCSWG), which includes public and private sector representatives from each of the 18 critical infrastructure and key resources (CIKR) sectors defined under the NIPP.[51] The CSCSWG meets monthly and offers a mechanism for public-private collaboration on cybersecurity initiatives, such as improving information sharing, considering private sector incentives for increased cybersecurity, and developing cybersecurity metrics that can be used by multiple CIKR sectors. As directed by the President's *Cyberspace Policy Review*,[52] the CSCSWG is currently assisting with the development of a National Cyber Incident Response Plan, which will provide a much-needed framework to improve public-private coordination in response to cyber incidents.

---

[49] Individual Federal agencies and organizations are responsible, in the first instance, for securing their own communications and information resources. For example, the Department of State (DOS) blocks 3.5 million spam e-mails, intercepts 4,500 viruses, and detects over a million external probes to its network in a typical week. DOS accomplishes this protection by implementing a matrix of technical, operational, and management security controls designed to thwart network threats, detect and mitigate vulnerabilities, and strengthen business operations.

[50] Other DHS agencies are engaged in cybersecurity activities. The U.S. Secret Service plays an extensive role investigating a wide array of cybercrimes. The Secret Service's Electronic Crimes Task Force brings together federal and non-federal law enforcement, academia, and the private sector to prevent, detect, and investigate attacks on critical infrastructures. *See* United States Secret Service website, http://www.secretservice.gov/ectf.shtml. The Office of Infrastructure Protection works with private sector providers of critical infrastructure and key resources to ensure that, along with a wide range of other risks, they address cybersecurity.

[51] Similarly, as more of the Nation's critical infrastructures have begun to adopt and deploy network-connected industrial controls, NCSD has substantially increased its collaborative efforts with industry on control system security, including the continued expansion of the Industrial Control Systems Joint Working Group (ICSJWG) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Each group follows a public-private partnership model and represents a growing area of collaboration.

[52] *See Cyberspace Policy Review*, *supra* note 42.

The Department of Justice (DOJ) conducts cyber investigations, enforces relevant criminal laws, and supports Intelligence Community efforts to identify and neutralize cyber threats. The Federal Bureau of Investigation (FBI) defends government, military and commercial networks by preventing and responding to cyber attacks, dismantling hostile computers/networks, sharing cyber intelligence and working with other federal agencies, foreign counterparts, and the private sector.[53] The FBI is the only federal agency with a legal mandate to investigate criminal intrusions and national security-related intrusions into government, military and commercial networks. This dual jurisdiction gives the FBI the ability to synthesize information across these distinct disciplines and to determine whether a network or computer intrusion is purely criminal or part of a state-sponsored intelligence operation. The FBI's Cyber Division works closely with its Counterterrorism, Counterintelligence, and Criminal Divisions to identify and neutralize hostile and illegal computer supported operations.

The FBI is the also Executive Agent for the National Cyber Investigative Joint Task Force (NCIJTF), which is an 18-member task force that has the capability to deconflict all ongoing investigations of federal, state, and local law enforcement and the Intelligence Community. Pursuant to National Security Presidential Directive (NSPD)-54/Homeland Security Presidential Directive (HSPD)-23, the NCIJTF serves "as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations."[54] The directives also task the NCIJTF with ensuring that "participants share the methodology and, to the extent appropriate, case information related to criminal cyber intrusion investigations among law enforcement organization represented in the NCIJTF." As such, the NCIJTF identifies, mitigates, and disrupts cyber threats by coordinating and integrating the counterintelligence, counterterrorism, intelligence, and law enforcement activities of member organizations.[55]

2. International Operations

The international community also plays a vital role in the U.S. Government's efforts to prevent, detect, and respond to cyber incidents. The Department of State has the statutory responsibility to coordinate U.S. international policy relating to cybersecurity.[56] In that role, the State Department hosts federal advisory committee meetings with the private sector to solicit their advice on U.S. positions on cybersecurity, as well as interagency meetings involving relevant federal agencies to formulate U.S. positions to be articulated internationally. It then

[53] For example, the FBI's Infragard Program attempts to promote information and intelligence sharing among businesses, academic institutions, state and local law enforcement agencies, and others in order to prevent hostile acts against the United States. *See* http://www.infragard.net/about.php?mn=1&sm=1-0.

[54] For a discussion of this classified directive, see "Bush Order Expands Network Monitoring," January 26, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html.

[55] Other Federal agencies have a cybersecurity role as well. The National Science Foundation (NSF) is doing research and development work in this area. The Department of Energy is working on measures to protect the national power grid, while the Department of the Treasury has an extensive cybersecurity role to protect financial transactions, such as its weekly sale of millions of dollars of bonds. NIST is actively developing technical standards for cybersecurity. Moreover, Federal agencies are improving the security of their own internal communications. The Cyberspace Policy Review has called for the establishment of a National Security Council directorate to coordinate many of these activities.

[56] *See* 22 U.S.C. § 2707 (2006).

leads U.S. delegations composed of agency and industry representatives to meetings at, for example, the International Telecommunication Union (ITU), the Organization for Economic Cooperation and Development (OECD), the Asia-Pacific Economic Cooperation forum (APEC), and the Inter-American Telecommunication Commission (CITEL). To give one example, the State Department leads U.S. delegations to Study Group 13 of the ITU Telecommunications Standardization Sector, which is devoted to developing standards for Next Generation Networks (NGN), including "built-in" rather than "bolted-on" cybersecurity standards for NGN broadband platforms.[57]

The State Department also organizes and hosts bilateral meetings with other countries on cybersecurity issues. It is also actively involved, in coordination with the appropriate federal agencies, in the development of international positions on national security, cyberterrorism, critical information infrastructure protection and law enforcement aspects of cybersecurity. In this capacity, it leads delegations to meetings of the North Atlantic Treaty Organization (NATO) and the Organization for Security Cooperation in Europe (OSCE), and the UN General Assembly where cybersecurity issues are discussed.

The Department of Justice has led an effort to expand the international network for quickly obtaining informal assistance from cyber investigators and prosecutors abroad so that electronic evidence is not lost. Through this network, known as the 24/7 High-Tech Crime Point-of-Contact Network, there are now 24-hour points of contact in over 50 countries capable of providing immediate assistance in preserving and obtaining electronic evidence. This network, along with incident-specific collaboration, has led to numerous successes in combating transnational cyber intrusions.

Similarly, DHS participates in the delegations led by the State Department to international meetings identified above, and frequently participates in the bilateral meetings on cybersecurity organized by the State Department. In addition, it engages bilateral and multilateral forums with international partners to address cybersecurity issues of mutual concern.[58] This includes collaborating with individual nations as well as groups of nations to build trust, share best practices, establish operational information-sharing relationships and related procedures, leverage capabilities, exchange expertise, and help other nations develop their own cybersecurity capabilities. NCSD works with international partners in a number of areas that range from computer security incident response team collaboration to cooperation on industrial control systems security. It regularly shares information with international government partners regarding best practices for engaging with industry. NCSD also facilitated international participation in Cyber Storms I and II, the U.S. national level cyber exercise series.[59]

---

[57] The Department of Commerce participates in State Department-led efforts at the ITU to help Developing Countries build capacity in cybersecurity. Commerce also provides courses in cybersecurity capacity at the United States Telecommunications Training Institute (USTTI).

[58] For example, the Meridian Conference and Process, which the United Kingdom initiated in 2005, aims to engage governments in cooperatively addressing Critical Information Infrastructure Protection (CIIP) issues from a global perspective. It explores the benefits and opportunities of cooperation between government and the private sector, and among governments internationally, and captures best practices from around the world.

[59] NCSD hosted an Observer Program during Cyber Storm II in which 14 nations participated. Planning work is currently underway on Cyber Storm III, which is scheduled for September 2010 and will include participants from Federal, State, and local governments, as well as industry and international partners.

DHS maintains strong collaboration with the Working Group of Key Allies, which is a partnership among Australia, Canada, New Zealand, the United Kingdom, and the United States whose mission is to collaborate on cybersecurity matters. The group's activities include:

- Real-time operational information sharing to enhance situational awareness, mitigate vulnerabilities, and manage incidents;
- Participation in cyber exercises to test and enhance existing processes and procedures for managing cyber events; and
- Coordination on cybersecurity policy and public affairs issues.

DHS also engages with the International Watch and Warning Network (IWWN), an organization of 15 member countries whose goal is to further international cooperation on cyber policy issues and incident response. The IWWN is composed of government cybersecurity policy makers and managers of computer security incident response teams with national responsibility. The IWWN's current focus is on improving operational collaboration through cooperation on cyber exercises.

C. **Existing Market Incentives for Commercial Communications Providers**

In light of near universal dependence on the Internet for business operations, all communications providers and users already have broad interests in network security. The revenue streams of communications providers, as well as those of businesses that rely on communications providers are at risk if operations are disrupted by cyber attacks. Many users in regulated industries are already subject to regulatory requirements for security and privacy. Nonetheless, even with the existing requirements and motivations, there is arguably a gap between the level of security the market currently provides and the level needed to protect NS/EP interests adequately.

To begin to address these gaps, the Cross-Sector Cyber Security Working Group (CSCSWG) recently completed a draft report stemming from a requirement under the Comprehensive National Cybersecurity Initiative to recommend a set of incentives, across all CIKR sectors, to drive improvement in the private sector's cybersecurity posture where market forces alone yield an insufficient value proposition. The report reflects discussions of CIKR sector participants in the CSCSWG and its Incentives Subgroup. It does not represent the official position of any Federal agency present in those discussions, nor does it represent an official position of any individual company. Rather, this document reflects CSCSWG participants' consideration of a broad range of incentives that may be applicable for, or within, CIKR sectors. We summarize the perspectives of this group here even though they have not yet been adopted as an official Administration position.

1. Communications Providers' Implementation of Cybersecurity Measures

End-users face significant challenges when it comes to selecting communications providers—they must weigh capabilities against costs and determine which provider can best meet their needs. This complex endeavor is made even more complicated when security is one of the capabilities that must be weighed. Some end users may not fully appreciate the importance of cybersecurity. However, even those end users who appreciate the value of

cybersecurity may not have the information they need to make an informed decision. End users must have the means to choose providers based on security as one factor. But it is also critical that State, municipal, and local government agencies have the ability to select providers that can satisfy their security needs.

NCSD's Outreach and Awareness Program is intended to raise the awareness of cybersecurity in general and to give end users more specific information to address their cybersecurity issues. NCSD's Outreach and Awareness program focuses on increasing cybersecurity and cybersafety awareness among small and medium sized businesses, educational institutions, home computer users, and the general public. It sponsors the annual National Cyber Security Awareness Month each October with public and private sector partners. The program also conducts on-going awareness campaigns throughout the year. Consistent with the Cyberspace Policy Review, the Outreach and Awareness program will work with its partners to enhance year-round awareness initiatives, including an increased focus on K-12 education. Informed and aware end-users should be more likely to seek out independent information regarding the cybersecurity options offered by communications providers.

2. Cybersecurity Best Practices Implemented by Communications Providers

Numerous cybersecurity best practices and standards are available to communications providers and private network operators. Many providers have leveraged these tools in building their security operations.[60] The information technology and communications sectors provide Internet routing, access, and connection services capabilities that support Internet backbone infrastructure, points of presence, peering points, local access services, and capabilities to direct Internet traffic. With regard to this function, several cybersecurity best practices are used across the sectors, including mitigation strategies designed to prevent a local or regional disruption from cascading and having national consequences. With regard to routing in particular, providers use protocols that re-route traffic when a transmission path is disrupted. Additionally, major providers have several backups for their routers in case the equipment fails. Network resilience is further enhanced by the multiplicity of peering arrangements and the geographic diversity of provider networks.

3. Wireless Network and Handset Features to Combat Cyber Attacks

Looking at wireless network and handset features from an end-user security point of view, defenses need to be provided from two major types of attacks:

- Protecting the end-user system and data from exploitation/attack; and
- Preventing the end-user system from becoming a part of the growing problem of botnets.

Each device and its supporting infrastructure typically has unique security capabilities that must be configured by the user or system administrator driven by the risk management profile of the user or enterprise. The level of sophistication of such security controls can vary

[60] Much of this information may have been previously provided to the FCC by the carriers in the context of their customer proprietary network information (CPNI) rulemakings over the past two years.

widely among devices and networks. The Broadband Plan should recognize and encourage the proliferation of industry best practices that effectively mitigate such cybersecurity risks.

4. Cybersecurity Education and Other Activities

To promote an adequate supply of trained cybersecurity professionals, Federal agencies support key education programs and training opportunities. For example, the National Science Foundation (NSF) and DHS sponsor the Scholarship for Service program, which is "designed to increase the cadre of federal information assurance professionals who protect the government's critical information infrastructure."[61] NSA and DHS co-sponsor the National Centers of Academic Excellence in Information Assurance Education and Centers of Academic Excellence research programs. These programs are designed to reduce vulnerability in our national information infrastructure by promoting higher education and research in information assurance.[62]

Efforts are underway to further secure Federal networks as well. OMB has required all federal agencies to deploy Domain Name System Security (DNSSEC) by December 2009.[63] The Domain Name System (or DNS) allows Internet users to resolve an alphanumeric website name (e.g., www.irs.gov) into the corresponding IP numerical address necessary to access that website. DNSSEC provides authentication to DNS lookups that mitigates certain DNS-based attacks and adds security to those operations. NTIA is taking steps to facilitate broader DNSSEC deployment by implementing DNSSEC at the authoritative root zone of the DNS, which is scheduled to be operational by mid 2010. NTIA has also approved for the implementation of DNSSEC within the U.S. top level domain (.us) and the domain utilized by institutions of higher education (.edu), which will become operational in 2009 and 2010 respectively. Also, as IPv6 implementation planning moves forward, federal agencies can anticipate the introduction of IPSec[64] in their networks, which will provide authentication, encryption and data integrity protection capabilities at the network layer.[65]

D. **The Commission's Role in Cybersecurity**

The Commission could reinforce its network security efforts in two ways. First, it could actively encourage telecommunications network and service providers to report basic information about network attacks and responses thereto, much as the Commission now requires telecommunications carriers to provide information on network outages.[66] Such reporting would provide valuable information to government and industry about the nature and scope of network attacks. As importantly, the prospect of public disclosure could induce service and network

[61] *See* OPM website, https://www.sfs.opm.gov.
[62] *See* NSA website, http://www.nsa.gov/ia/academic_outreach/nat_cae.
[63] *See* Memorandum for Chief Information Officers, "Securing the Federal Government's Domain Name System Infrastructure," M-08-23 (August 22, 2008), http://www.whitehouse.gov/OMB/memoranda/fy2008/m08-23.pdf.
[64] Internet Protocol Security (IPSec) is a suite of protocols that integrates security features into Internet Protocol (IP) communications.
[65] *See* CIO Council, "Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government" (May 2009), http://www.cio.gov/library/documents_details.cfm?id=Planning%20Guide%20/%20Roadmap%20Toward%20IPv6%20Adoption%20in%20the%20U.S.%20Government&structure=Enterprise%20Architecture&category=IPv6.
[66] *See* 47 C.F.R. §§ 4.1 *et seq.* (2008).

providers to comply with established best practices to deter attacks. It could also spur a "race to the top" where security would become a prominent part of firms' competition for customers.[67]

Second, the Commission could supplement existing federal government efforts to educate consumers about network threats and the ways that they can combat those threats. As described previously, the NCSD has a number of programs in place to educate consumers. Effective collaboration among the FCC, NCSD, and other partners on consumer awareness activities can lead to better informed and aware end-users, who will be better equipped to seek and adopt cybersecurity options offered by communications and applications providers.

E. **The Federal Role in Cybersecurity**

Government has a clear and long history of shared responsibility for coordination, restoration, and reconstitution of NS/EP telecommunications services or facilities. In order to prevent cyberspace from becoming a safe haven for criminals and terrorists, capabilities which allow law enforcement to conduct electronic surveillance without compromising the end-user system and data must be conceived of and designed in conjunction with cyber security. In developing the National Broadband Plan, the Commission should endeavor to provide sufficient information about the future evolution of communications networks to permit an assessment whether existing laws and regulations are adequate to maintain electronic surveillance capabilities and protect civil liberties on those emerging networks.

Government can also play a key role in defining cybersecurity obligations for applications and service providers, and by establishing basic rules, guidelines, and best practices necessary to protect individual rights, while meeting national security needs. The best result would be for government to avoid being overly prescriptive, giving wide discretion to the private sector to develop innovative and effective security measures and strategies to meet cybersecurity obligations. Finally, government should continue to share its accumulated experience and expertise in cybersecurity matters in public-private collaborations to develop improved security protocols and standards, and industry best practices. As a collaborator in cybersecurity activities, government should inform and not direct its partners, and assist and not prescribe overly specific measures as to how applications and service providers meet cybersecurity obligations.

The National Broadband Plan should acknowledge the contributions made by organizations in cybersecurity research and training activities as well, and highlight the critical role that public/private partnerships play in improving our national cybersecurity posture.[68] It should identify organizations working on security concerns directly related to broadband network operations in cyberspace, and those involving cyber attacks launched over broadband networks. Finally, the Plan should recognize the critical responsibility that all organizations have in promoting a consumer awareness of the potential risks and measures that consumers can take to mitigate cyber threats.

---

[67] *See* Transcript of FCC National Broadband Plan Workshop on Cyber Security, at 75-76 (Sept. 29, 2009), http://www.broadband.gov/docs/ws_26_cyber_security.pdf.

[68] "Industry and governments share the responsibility for security and reliability of the infrastructure and the transactions that take place on it and should work closely together to address these interdependencies." *See Cyberspace Policy Review*, *supra* note 42, at 17.

F. **Conclusion**

The Nation relies increasingly on the Internet as a vehicle for innovation, economic competitiveness, national prosperity, and a tool for efficiency, transparency and accountability in government. Along with the clear benefits, come a range of emerging risks and growing threats by a host of adversaries, including organized and individual criminals, nation-states and terrorists. The threats to cyberspace are real, growing, and evolving. Given the current threat environment, the Administration strongly endorses the inclusion of cybersecurity elements in the National Broadband Plan being developed by the FCC. The National Broadband Plan should identify measures taken to enhance cybersecurity and recognize the responsibility shared by both public and private sector interests in creating effective, coordinated, and cooperative strategies to mitigate the cyber threat.

V. **A PATH FORWARD**

The National Broadband Plan will be an important contribution to Federal efforts to expand the availability and adoption of broadband services. Emergency responders and other public safety agencies can benefit greatly from broadband deployment. The Plan at its core should recognize the layered model that has allowed the Internet to become a transformative technology that empowers people around the globe, spurs innovation, facilitates trade and commerce, and enables the free and unfettered flow of information. Incorporation of this model into the Plan will not only provide a framework to foster continued innovation, but will also address important public safety, national security, and homeland defense priorities.