UNITED STATES DEPARTMENT OF COMMERCE
The Assistant Secretary for Communications and Information
Washington, D.C. 20230

December 10, 2009

The Honorable Julius Genachowski
Chairman
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: National Broadband Plan, GN Doc. No. 09-51, NBP Public Notice #8

Dear Chairman Genachowski:

The National Telecommunications and Information Administration (NTIA) welcomes the opportunity to express the Administration's views on the public safety, homeland security and cybersecurity elements of the National Broadband Plan ("Plan").[1] The Plan 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 letter and the attached 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.

Indeed, with the advent and adoption of mobile and fixed broadband Internet communications, we can imagine a world where the following is possible:

- Fire officials viewing different angles of a fire simultaneously, from remote cameras deployed around the scene of an incident.
- FEMA accessing detailed infrastructure plans in real-time and sharing them, as authorized, with other responding agencies.
- The FBI sharing data with local law enforcement over secure virtual private networks.
- 911 operators gathering pictures of an accident victim and making them available to arriving emergency medical personnel ambulance, so that they are prepared to provide assistance upon arrival and then forward informative pictures to the hospital in-route.
- Government agencies and private sector network operators sharing data in real time about evolving threats to networks in order to thwart cyber attacks before they can spread

[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 attachment provides responses to questions posed in the Public Notice.

We are encouraged by early experiments and demonstration projects along these lines and they are really just a small fraction of what should be possible nationwide.

A Layered, Open-Platform Design Strategy for Public Safety Communications, NG911, and Cybersecurity

We are in an era of decentralized communications characterized by innovation at the edges 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 at once so complex, so incompatible with traditional command-and-control regulation, and so 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 this 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

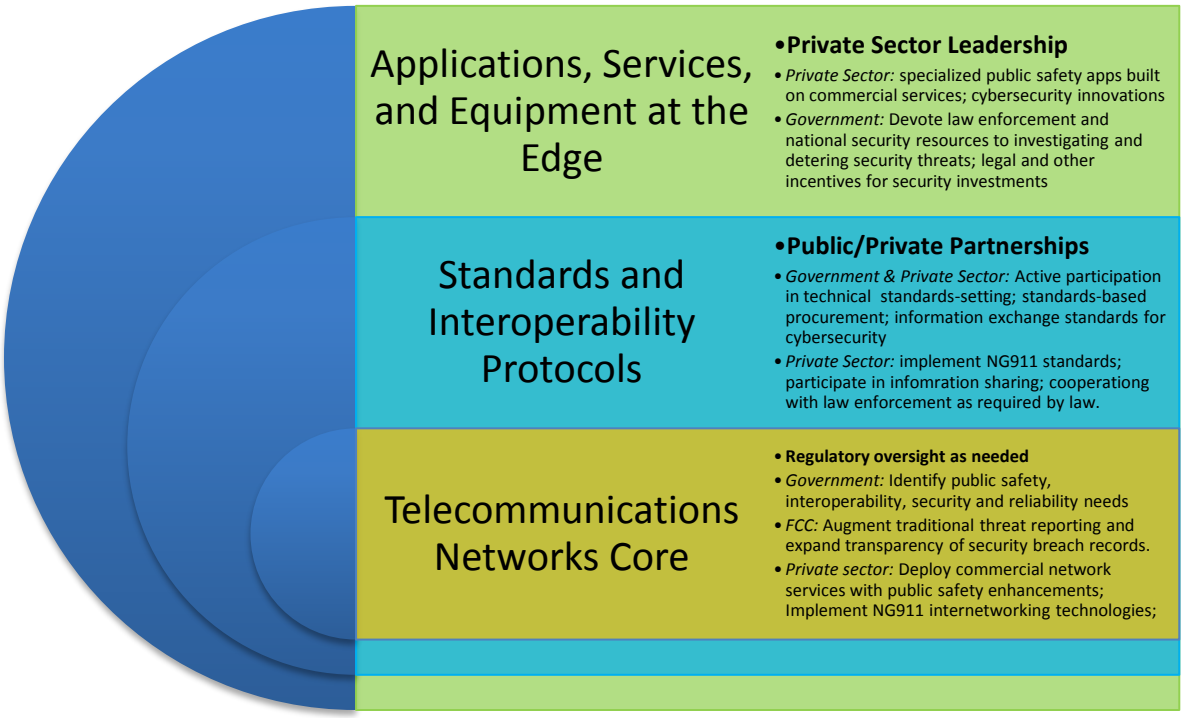

Figure 1 - Framework for Internet Development as It Relates to Public Safety, NG911 and Cybersecurity Responsibilities

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.

Public Safety Goals of Interoperability, Robustness, Reliability, and Prioritization Are Key

Public safety and emergency responders envision near and long-term uses of broadband applications that will improve situational awareness, provide real-time retrieval of critical data, and enhance collaborative decision-making. Guided by the lessons learned from the September 11th attacks, Hurricane Katrina and other natural disasters, the Administration supports actions that can result in interoperable, innovative, effective, reliable, and affordable public safety communications systems. To best achieve this goal, we should look to public-private partnerships, which is how this country has met so many of its great challenges, in order to assist public safety's shift away from continued reliance on a siloed, switched network services model, wholly-dedicated devices, and proprietary systems, and towards more modern networks and devices that solve problems while maintaining the high standards that public safety demands.

The Commission should explore the extent to which public safety can use commercial telecommunications networks, coupled with customized end user devices, to meet its unique needs. In so doing, the Commission should take into account the analyses of public safety communications' strengths and weaknesses conducted in the aftermaths of 9-11 and Hurricane Katrina. 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.[2] 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.[3]

During emergencies, local, state and federal public safety agencies have historically been given highest priority access to wireline and wireless switched networks. The need to assure access will be every bit as great on new IP-based networks, but the technical means of assuring priority on new Internet services will be different. In some cases access guarantees may be best met by using devices that can seek out available capacity on a variety of different networks. Putting public safety communications at the top of the queue is of little value if the entire network has been disabled. We must affirm our commitment to network availability for public safety users under adverse situations, but be creative in exploring the best means to satisfy this goal. In the same vein, the Plan should recognize that certain physical diversity, redundancy, reliability, and security aspects of public safety services separate them from traditional

[2] *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.
[3] *The Federal Response to Hurricane Katrina: Lessons Learned*, Chapter 5, § 3 (Feb. 23, 2006), *available at* http://library.stmarytx.edu/acadlib/edocs/katrinawh.pdf.

commercial network service offerings. For example, public safety networks have demanding requirements for hardening cell sites and other facilities to ensure network survivability.[4]

The use of standards-based and vendor-neutral technologies will promote network connectivity and spur the deployment of innovative applications and services on more affordable devices. Open technical standards and protocols will facilitate the delivery of wired and wireless technologies that will promote compatibility and interoperability across agencies, jurisdictions, and communities in a manner that helps them leverage legacy systems as they migrate towards newer technologies.[5] Ultimately, the Plan must identify both what is unique about public safety requirements, along with those needs that can be met through creative configuration of commercial network services.

Finally, the Plan should note the need for flexible and modular funding models that satisfy public safety broadband needs for interoperable, mobile, wireless services, yet avoid a "one-size-fits-all" approach. Numerous existing models to consider include state-wide systems, fee-for-service systems, and systems-of-systems approaches. The Plan should identify responsibilities for managing the various phases of the build out, including regulatory and contracting oversight.[6]

Federal and State Agency Efforts to Improve E911 Services

The National Broadband Plan should take notice of Federal and State efforts to improve E911 networks and call centers and build on the ICO's work to deploy NG911 networks. In the broadband network of the future, the general public must be able to send 911 emergency messages from any wired or wireless device. The emergency services community should be able to leverage advanced call-delivery and other functions through new internetworking technologies, based on open standards, to provide a complete voice, data and video link between the 911 caller and the first responder.[7] Consistent with the layered approach discussed above, E911 improvements should focus on innovative developments at the telecommunications network core, designed to handle traffic from feature-rich end user devices at the edge of networks, all supported by technical standards and protocol development activities. The Commission should look to maximize the information exchange potential of E911 services based on use of Internet standards, setting a high bar for what can be achieved.

---

[4] Public safety networks must include redundancy and diversity elements to handle traffic during outages or emergencies.

[5] To that end, the 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.

[6] The Plan should contemplate demonstrations of innovative strategies for broadband implementation in the 700 MHz and other bands, to the extent that such strategies are consistent with the overall goals articulated here. *See 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).

[7] Trends in personal communication technologies are accelerating the obsolescence of the current E911 system. The current circuit-switched infrastructure of the E911 network cannot handle digital data (*e.g.*, text messages, photographs, and video) from the communication devices now commonly used by the public.

A recent study by the National E911 Implementation Coordination Office (ICO), managed by NTIA and the Department of Transportation's National Highway Traffic Safety Administration (NHTSA), found that NG911 networks could offer significantly higher value over current 911 implementations, at similar costs, regardless of the level of coordination and cost sharing involved.[8] The ICO has developed "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."[9]

A Shared Responsibility for Cybersecurity

Along with the clear benefits and growing utility afforded by cyberspace, comes 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 gained 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 strategies in both the government and the private sector.

Public and private sector interests 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 work together to improve their own cybersecurity and that of our Nation."[10] 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. Applications providers and network operators can utilize this experience and knowledge as they continue to develop innovative features and/or operational procedures that further enhance the security of their products and services.[11]

---

[8] Congress established the ICO in 2004. *See* ENHANCE 911 Act of 2004, Pub. L. No. 108-494, § 104, 118 Stat. 3986, 3987 (codified in 47 U.S.C. § 942 (2006)). In 2008, Congress directed the ICO to develop a national plan for migrating to an IP-enabled emergency network. *See* New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. No. 110-283, § 102, 122 Stat. 2620, 2623 (codified in 47 U.S.C. § 942(d)).

[9] 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 .

[10] "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..

[11] The attachment describes Federal agency activities to identify and mitigate cyber threats, and collaborative efforts to share critical information with industry and the security research community.

Tracking the layered approach discussed above, at the Applications, Services, and Equipment layer, the private sector must lead in developing innovative security strategies and protection technologies. Here, the key government role is to assure vigorous domestic law enforcement and appropriate national security defensive and offensive postures.[12] 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.

The Standards and Protocol 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 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.[13]

In the Telecommunications Networks Core there is a long history of collaboration among the nation's communications infrastructure providers. The National Coordinating Center for Telecommunications (NCC), for example, 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 Commission's Role in Cybersecurity. Charged with "regulating interstate and foreign commerce in communication by wire and radio . . . for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communication,"[14] the Commission plays a critical role in protecting the security and integrity of the Nation's communications infrastructure. To date, the Commission has addressed network reliability and cybersecurity concerns through collaboration, rather than by imposing particular security mechanisms or arrangements on network and service providers.[15] Such mandates would likely discourage the innovation that is needed to keep pace with the ever-increasing range of cyber attacks.[16]

The Commission should continue with this collaborative approach, as opposed to overly prescriptive mandates. The Commission could reinforce its cybersecurity efforts in two

---

[12] The legal system must safeguard personal privacy, provide adequate consumer protection, and prevent unwarranted government intrusion on individual rights.

[13] In most cases, private sector-led standards setting is still appropriate, but input from appropriate Federal agencies – the National Institute of Standards and Technology and the Department of Homeland Security – will be vital to define requirements and set priorities.

[14] 47 U.S.C. § 151 (2006).

[15] *See, e.g.*, Charter of the FCC's Communications Security, Reliability and Interoperability Council, http://www.fcc.gov/pshs/docs/advisory/csric/csric-charter-final.pdf.

[16] *See* Transcript of FCC National Broadband Plan Workshop on Cyber Security, at 68-71 (Sept. 29, 2009), http://www.broadband.gov/docs/ws_26_cyber_security.pdf.

additional ways. First, it could actively encourage the reporting of basic information about network attacks and responses thereto. Second, it could supplement existing federal consumer education efforts. For example, in the Department of Homeland Security, the National Cyber Security Division's (NCSD) Outreach and Awareness Program attempts to raise awareness of cybersecurity among small and medium-sized businesses, educational institutions, and the general public, and to give those groups more specific information to address their cybersecurity issues. Effective collaboration 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.

A 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. It can also play a key role in defining cybersecurity obligations for applications and service providers, by establishing basic rules, guidelines, and best practices necessary to protect individual rights, while meeting national security needs. In so doing, government should avoid being overly prescriptive, but should instead give the private sector discretion to develop innovative and effective security measures and strategies to meet their cybersecurity obligations. Finally, government should continue to share its accumulated experience and expertise in cybersecurity matters in public-private collaborations.

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

Thank you for your consideration of these views.

Respectfully submitted,

/s/
Lawrence E. Strickling

cc: The Honorable Michael J. Copps
The Honorable Robert M. McDowell
The Honorable Mignon L. Clyburn
The Honorable Meredith Attwell Baker
Marlene H. Dortch, Secretary