Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan	)	GN Docket Nos. 09-47, 09-51, 09-137
	)	
	)	PS Docket Nos. 06-229, 07-100, 07-114
	)	
	)	WT Docket No. 06-150
NBP Public Notice #8	)	
	)	CC Docket No. 94-102
	)	
	)	WC Docket No. 05-196
	)	

VERIZON AND VERIZON WIRELESS

COMMENTS – NBP PUBLIC NOTICE #8

Michael E. Glover
Of Counsel

Karen Zacharia
Mark J. Montano
VERIZON
1320 North Courthouse Road
9th Floor
Arlington, VA 22201
(703) 351-3058

John T. Scott, III
VERIZON WIRELESS
1300 I Street, N.W.
Suite 400-West
Washington, DC 20005
(202) 589-3760

November 12, 2009

Attorneys for Verizon and Verizon Wireless

TABLE OF CONTENTS

I. Public Safety Mobile Wireless Broadband Networks..... 2

II. NG911..... 9

III. Cybersecurity 13

INTRODUCTION

Verizon and Verizon Wireless[1] have long been actively engaged in the public safety and cybersecurity issues on which the Commission has requested comments to prepare its National Broadband Plan.[2] These efforts include serving public safety agency customers, and collaborating with government entities on developing next generation 911 services (NG911), as well as preparing for and responding to cyber attacks. All providers of communications services, large and small, should be encouraged to similarly participate in these important collaborative efforts, which will directly benefit emergency responders and other public safety agencies and enhance the security of the nation's broadband networks.

To help achieve these objectives, the Commission should take the following concrete steps. First, the Commission should encourage Congress to designate the 700 MHz D block spectrum for public safety use to ensure that public safety organizations' expanding communications needs are met. The Commission should also ensure that as new public safety networks are developed, they are interoperable.

Second, the Commission should encourage the completion of NG911 standards and resolve any open regulatory questions that currently hinder the development of these standards. The substantial work to date on NG911 demonstrates what can be achieved when public and private entities work together on a solution.

---

[1] With the exception of Verizon Wireless, the Verizon companies participating in this filing are the regulated, wholly owned subsidiaries of Verizon Communications Inc. ("Verizon").

[2] *Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan*, NBP Public Notice # 8, DA 09-2133 (Sept. 28, 2009) ("Public Notice").

Third, the Commission should leverage the cybersecurity expertise developed by other sectors of the government and coordinate those efforts across agencies. The Commission should also continue to foster public-private collaboration. The Commission recently re-chartered the Communications Security, Reliability, and Interoperability Council (CSRIC), which could be tasked with identifying cybersecurity best practices. Best practices provide companies with the flexibility to respond to ever evolving cybersecurity threats. At the same time, the Commission should avoid adopting restrictive network management rules that could hinder the ability of broadband providers to respond quickly to such threats.

DISCUSSION

As requested in the Public Notice, Verizon and Verizon Wireless provide the following responses to the Commission's questions:

I. Public Safety Mobile Wireless Broadband Networks

A. How are public safety agencies making use of broadband networks today?

The public safety community uses Verizon Wireless' services on both a day-to-day basis and in the aftermath of natural/man-made disasters. First responders use Verizon Wireless' voice and data communications products and services to communicate with each other in the field; to access important information contained in local, state and federal crime database systems; to manage their field forces through fleet monitoring capabilities; and to access many other applications that help first responders do their jobs securely and effectively. Commercial wireless services are a key tool used by local, state, and federal governments to reduce operational costs, increase productivity, and ensure public safety responsiveness. Here are just a few examples of how the public

safety community benefits from the availability of advanced wireless communications services:

- A large east coast police department recently supplied every officer in the field with a BlackBerry® smartphone equipped with PocketCop® and GPS tracking capability. PocketCop® is an application developed by Bio-Key, a leader in biometric security, that provides law enforcement with a fully integrated and secure mobile data system. It allows patrol officers to remotely access a variety of law enforcement databases to do such things as check vehicle registrations, run warrant checks and access prior criminal history. The built-in GPS capability assists police dispatchers in responding to incidents by tasking nearby officers.

- A medium-sized city police department uses 1,800 Windows Mobile devices equipped with Watson software that enables access to a host of information over the Internet without using a web browser. With the device, police officers can access information in the National Crime Information Center database, literally putting criminal records in the palm of their hand. GPS is used to map out potential crime patterns and to stimulate proactive policing.

- A small midwest police department has supplied their field officers with ruggedized "push to talk" (PTT) devices that are equipped with VZ Navigator℠ and Verizon Wireless' custom Field Force Management application. These devices support the department's command and control and task force dispatch functions. They are used to schedule and dispatch jobs, receive job and task force reports, as well as to locate remote employees. Using these devices and Verizon

Wireless' advanced evolution-data optimized (EVDO) network, the department has improved coordination and communications.

These services are all supported on Verizon Wireless' Third Generation (3G) mobile broadband network, which utilizes advanced Code Division Multiple Access (CDMA) EVDO technology. This 3G network has been deployed throughout the nation, and currently covers more than 95% of the U.S. population.

Verizon Wireless' goal is to provide an array of voice and data communications products and services that allow public safety entities to perform their duties more effectively and efficiently. In addition, because land mobile radio (LMR) systems continue to play a large role in emergency communications, Verizon Wireless recently launched an interoperability tool that allows organizations, including public safety entities, to integrate Verizon Wireless' PTT service with their existing LMR systems to create a broader LMR footprint that includes Verizon Wireless' network. This solution can help public safety entities reduce the costs associated with expanding LMR systems for more effective use of budget dollars; free up capacity on the radio network by moving certain user groups to the push-to-talk service; implement a back-up solution in case of an LMR outage; and introduce additional Verizon Wireless productivity tools such as Field Force Manager for mobile resource management, VZ Navigator^{SM} for turn-by-turn navigation, and mobile e-mail.

Verizon Wireless also has worked with various community governments and organizations to provide specialized services to those communities. For example, through an arrangement with the City of Chicago, Verizon Wireless provides free 311 non-emergency public service calls to customers using its service within the city limits.

E. We seek comment on what particular mobile wireless broadband needs could be satisfied by commercial broadband service providers in the short term and over the long term. Are there any assessment studies or field trials that show areas in which next generation mobile networks (4G) meet or do not meet Public Safety requirements?

As already noted, many of public safety's current emergency communications needs can be met with existing commercial broadband networks like Verizon Wireless' advanced 3G network. These networks support a variety of advanced voice and data solutions. In the future, however, first responders may benefit from access to a greater array of broadband data applications, such as video applications that will enable them to better assess an emergency situation and respond accordingly. The Fourth Generation (4G) wireless networks that commercial wireless providers are currently preparing to deploy will be better able to support these enhanced capabilities, particularly if providers' hands are not tied in effectively managing these networks and if providers continue to have the incentive and ability to develop and deploy more advanced networks and technologies. Verizon Wireless, for example, is planning to deploy an advanced 4G network utilizing Long Term Evolution (LTE) technology beginning in 2010. This 4G network will be better able to support the types of advanced communications capabilities that the public safety community may demand, as well as many other customer segments.

However, some state and local officials have concluded that dedicated public safety networks may be required in some areas to ensure that public safety's critical needs are met. As a result, we expect future emergency communications needs to be met through a combination of commercial and dedicated broadband mobile networks. Importantly, the nation's leading public safety organizations have endorsed LTE (or 4G)

as the air interface standard for 700 MHz public safety broadband networks.[3] By adopting the same technology standard that will be widely deployed by commercial operators, the public safety community leverages significant economies of scale and helps ensure interoperability across the country.

The National Public Safety Telecommunications Council (NPSTC) has developed a framework of minimum operational requirements that would support nationwide roaming and interoperability among public safety users. Verizon Wireless supports the establishment of a uniform framework for any regional public safety networks. The Commission should establish conditions for the buildout of regional public safety broadband networks on the use of LTE and compliance with an agreed upon set of operational requirements, perhaps modeled on the NPSTC framework. This would allow state, local, and regional authorities to build and operate networks on a network-of-networks basis.

G. What actions must the Commission or other entities take to ensure interoperability among public safety broadband systems?

The Commission's allocation of the 700 MHz band has made much needed spectrum available to meet growing customer demand and to provide for the introduction and growth of new wireless services. The 700 MHz auction was a tremendous success, raising nearly $20 billion for the U.S. Treasury and licensing new spectrum to meet growing consumer demand and to provide for the introduction and growth of new wireless services. However, in order to realize the full panoply of opportunities inherent

---

[3] *See Public Safety and Homeland Security Bureau Seeks Comment on Petitions for Waiver to Deploy 700 MHz Public Safety Broadband Networks*, Public Notice, 24 FCC Rcd 10814, App. A at 7 (2009) (noting support from APCO, NENA, NPSTC, and the PSST).

in this spectrum, the Commission needs to resolve the question of what to do with the D Block. Verizon Wireless urges the Commission to encourage Congress to designate this spectrum for a nationwide public safety network. Our nation's first responders require a modern broadband network that ideally is interoperable across the nation and can support the full panoply of innovative applications that help these men and women best do their jobs.

The Commission can help to address this national security imperative by adopting a proposal recently put forward by the public safety community. Led by the Major Cities Chiefs, the Association of Public Safety Communications Officials International, the National Emergency Number Association, and the Public Safety Spectrum Trust, this proposal would ensure that control over the process remains in the hands of those that best understand public safety's needs – i.e., state and local law enforcement and first-responder agencies. This approach would ensure that public safety providers receive the services and applications they require, while benefiting from the continuing investments and innovations of commercial carriers. It has four key, interdependent principles, which the Commission can work with Congress to accomplish.

First: the FCC should encourage Congress to reallocate the D Block for a nationwide public safety network. Providing public safety providers with both access to sufficient spectrum *and* direct control over its use would ensure that the D Block is used to meet public safety providers' expanding communications needs.

Second: the Commission should establish rules that facilitate the deployment of dedicated and/or shared regional networks that will enable state and local public safety

entities to more effectively consider local factors such as geography, population distribution, public safety capacity needs, and available existing commercial networks.

Third: the Commission should adopt a national technical framework that will ensure nationwide interoperability. While establishing local or regional networks may be the best way to satisfy diverse public safety needs, letting many diverse networks develop independently without any guiding national principles would repeat the mistakes of the past. This problem can be avoided by establishing national technical standards (including LTE as the common air interface) that ensure these IP networks can work together as one.

Fourth: public safety entities should be free to select the commercial partner or partners of their choice, using an RFP process or similar competitive approach. Local or regional partnerships that are tailored specifically to meet the needs of individual public safety agencies across the country are more likely to succeed than attempting to establish a single national partnership through an auction, which would require public safety entities to commit to a single model that may not satisfy local agencies' needs. Establishing a national plan that follows these principles, and working with Congress to provide state and local governments with federal funding to implement the plan, will put the country in the best position to address emergency communications needs. Public safety agencies get control over use of the spectrum, control over how the networks are built, and control over who they partner with, subject only to requirements intended to ensure nationwide interoperability of the resulting networks across states or regions. By partnering with the private sector, these agencies leverage the tremendous investment and innovation in networks that have already been made and will continue to be made,

eliminating significant costs for state and local government. This approach would best meet the urgent need to achieve interoperable public safety networks.

II. NG911

A. What are the broadband infrastructure requirements necessary to support deployment of NG911 capability?

For NG911 to work efficiently, one platform should serve the needs of wireless and landline users. To support these users, the network should have the capability to send and receive multimedia communications (i.e., voice, video, text, data, etc.). The network infrastructure should be able to efficiently use its bandwidth when managing high volumes of traffic, which would enable Public Service Answering Point (PSAP) call takers to manage emergencies more effectively. Managing the multimedia platforms requires a robust network consisting of common national network elements, vendor-agnostic equipment and an IP network-centric architecture. Moreover, ensuring that providers have flexibility to manage their network effectively and the ability and incentive to increase the capabilities of their networks will further this goal.

B. Have NG911 technical standards been completely defined? If not, what has been done and what remains outstanding? Where is the associated equipment in the development pipeline?

While NENA (National Emergency Number Association), IETF (Internet Engineering Task Force), ATIS (Alliance for Telecommunications Industry Solutions), 3GPP (3rd Generation Partnership Project), and others continue to work on NG911 standards development, a complete set of defined standards has not been completed at this time. Examples of issues being addressed include:

- Next Generation Emergency Services Locations Standards
- NGN/IMS Emergency Call Processing

- Ingress SIP Interface Specifications between IP Originating Networks and NG Emergency Services Networks
- NGN 911 Service
- Support of Emergency Telecommunications Services in IP Networks
- VoIP and Multimedia Services in Next Generation Networks
- Coordination of NG emergency Services Standards
- Next Generation Transition Planning recommendations
- Issues Related to Call Delivery from VoIP Sources
- Network Interface to IP-capable PSAP
- Best Current Practices for Communications Services in support of Emergency Calling
- Framework for Emergency Calling using Internet Multimedia
- Issues related to Location Hiding
- Security Threats and Requirements for Emergency Call Marking and Mapping.

These organizations host (with support from multiple PSAPs, network providers, and equipment manufacturers) working groups that hold periodic meetings and conference calls to continue the development of recommendations and standards to support NG911. Verizon and Verizon Wireless are actively engaged with various groups in these efforts.

C. To what extent are NG911 and near-NG911 technologies and services being deployed today? What states/regions/municipalities have already deployed these technologies and services or are on a path to doing so in the near-term? What factors have encouraged these deployments?

The near-NG911 technologies being deployed today include PSAP equipment that is IP-enabled for Emergency Call delivery. However, the IP-enabled PSAPs still require traditional TDM telephony for emergency call delivery to the PSAP. In addition, deployments that support a near-NG911 technology provide IP Selective Routing to replace TDM Selective Routing currently deployed in some PSAPs.

With respect to near-NG911, Verizon offers VoIP services that use a version of the NENA i2 architecture, which is used to support the interconnection of VoIP domains with the existing Emergency Services Network infrastructure in support of the migration

toward end-to-end emergency calling over the VoIP networks between callers and PSAPs.

D. Are there regulatory roadblocks that may be restricting more vigorous NG 911 deployment? Which of these are within the Commission's jurisdiction and what actions should the Commission take in this regard?

The Commission should provide clarity on outstanding Internet Protocol (IP) enabled service issues. As Verizon has explained elsewhere, the Commission should rule that all VoIP and IP-enabled services, regardless of the provider or technology employed, are jurisdictionally interstate services subject to the Commission's exclusive jurisdiction, and not to more than 50 different sets of economic regulation.[4] But even after ruling on its jurisdiction, the Commission should also exercise caution in reviewing requests to extend regulation to these new technologies. Hasty extension of regulatory requirements would hamper the existing development and maintenance of voluntarily negotiated, arms-length agreements which specify how 911 interconnection should occur, given the specific networks and circumstances present in a particular jurisdiction.[5]

Furthermore, the Commission should ensure that network operators have the flexibility they need to effectively manage their networks, and should not adopt net regulations that undermine providers incentive to invest in and deploy advanced, intelligent networks and other technologies that are better able to address public safety concerns.

---

[4] Comments of Verizon and Verizon Wireless, *Developing a Unified Intercarrier Compensation Regime*; *Intercarrier Compensation for ISP-Bound Traffic*; IPEnabled Services, et al., WC Docket Nos. 05-337, 03-109, 06-122, 04-36; CC Docket Nos. 96-45, 99-200, 96-98, 01-92, 99-68, at 5-21 (Nov. 26, 2008).

[5] In addition, NENA's Next Generation Partnership is working with the Department of Transportation to identify regulatory roadblocks.

E. What technologies are available or under development in the NG911 environment to facilitate automatic location identification? How can this data be made useful to Public Safety Answering Points (PSAPs)?

Location-to-Service Translation protocol (LoST), Location Verification Function, (LVF), and Location Information Service (LIS) are inter-related technologies supporting the location of an Originating Emergency Service Event and will be delivered to the PSAP with the Originating Emergency Event setup. The standards for these calls will be deployed as part of the NENA i3 model.

ATIS's Emergency Services Interconnection Forum (ESIF) has prepared two Technical Reports that describe the location acquisition and location conveyance functions within access networks. These documents analyze different protocols and include a recommendation for consideration by standards groups such as the IETF. The Technical Reports' recommended protocols can be used to communicate with a Location Information Server so that the specific location of the device can be downloaded and stored in the device itself. This location information on an emergency call would be used to interface with a NG911 Emergency Call Routing Function to determine the target PSAP URI for routing NG911 calls. The location information conveyed to the PSAP in the incoming SIP signaling would be useful to determine the location of the calling party and responding to the incident.

F. What does the public safety community, including PSAPs, need to do to enable emerging internet applications that reliably deliver voice, video and data information to PSAPs? What is the best architecture and means to accomplish this?

The public safety community should support industry standards to enable emerging internet technologies solutions to support an inoperable, secure and robust environment.

The PSAPs should work jointly with the state, communities of governments, counties and carriers to have a secure IP-based network that can both receive and send packets of data and support the current voice structure. The public safety community, including PSAPs must proceed to upgrade their current legacy PSAP systems to accommodate a SIP interface. This is a fundamental requirement to begin the transition to a NG911 infrastructure. The public safety community needs to work closely with their 911 service providers to provide an ESInet architecture and deploy the latest NG911 security recommendations now being prepared by NENA.

III. Cybersecurity

A. What type of computer-based attacks against government or commercial computer systems or networks (i.e. cyber attacks) are occurring or are anticipated to occur, and what are other federal agencies, commercial, and other entities doing to prevent, detect and respond to cyber attacks?

Commercial[6] and government networks that interface with public networks are likely subject to denial of service attacks, unsolicited email (spam), phishing, spyware and other unauthorized programming, and other malicious attacks. The operators of these networks likely employ widely available security programs and firewalls to detect, remedy and mitigate such events and/or work with security services providers, including Verizon, and law enforcement to detect, remedy, and mitigate such events.

Federal agencies and other government entities are taking proactive measures to protect themselves from cyber attacks. For example, the Office of Management and Budget (OMB) has recently announced plans to use scanning software government-wide,

---

[6] Verizon recently described to the Commission some of its efforts to protect its own internal networks. *See* Ex Parte Letter from Nneka Ezenwa, Verizon, to Marlene Dortch, FCC, *A National Broadband Plan for Our Future*, GN Docket No. 09-51 (Oct. 29, 2009).

which would enable it to scan every computer and server connected to a government network at least every 36 hours.[7] The results will then be ranked against eight security factors, and agencies will be scored based on how well they mitigate risks. Furthermore, the Department of Homeland Security (DHS) Secretary Janet Napolitano recently announced DHS's new authority to recruit and hire up to 1,000 cybersecurity professionals over the next three years to fulfill critical cybersecurity roles, including cyber risk and strategic analysis; cyber incident response; and vulnerability detection and assessment.[8]

B. How are other federal agencies of the United States and other governments collaborating with the communications segment to prevent, detect, and respond to cyber attacks?

Verizon, like many other communications companies, has a close working relationship with the myriad federal agencies and governmental bodies that have asserted responsibility for cybersecurity. This collaboration between the government and the private sector has significantly improved the United States' ability to respond to cyber attacks. In light of the existing efforts by numerous agencies and government bodies on issues of cybersecurity, the Commission could play an important role in cybersecurity by leveraging those efforts and fostering inter-agency coordination to focus on protecting against and responding to cyber security attacks. It is especially important that new cybersecurity requirements not be placed on private entities by the Commission unless

---

[7] *See* Jason Miller, *Agency Cybersecurity Reporting to Get Makeover*, http://www.federalnewsradio.com/index.php?nid=35&sid=1798890 (Oct. 30, 2009).

[8] *See Secretary Napolitano Announces New Hiring Authority for Cybersecurity Experts*, News Release, http://www.dhs.gov/ynews/releases/pr_1254411508194.shtm (Oct. 1, 2009).

and until there is a holistic understanding of the need for such measures in the broader context of overall government agency and legislative activity in this area.

Moreover, restrictive new regulation of network management practices would undermine the quality and security of consumers' services and the important national interest in more effective cybersecurity. Government policies that create uncertainty about permissible network management practices should also be avoided because they could undermine the ability of broadband providers to respond quickly to new and emerging cybersecurity threats. Instead, the Commission should leave it to engineers and network managers – not lawyers or regulators – to determine the practices that best serve consumers' interests. Verizon is working with the following governmental groups in their cybersecurity efforts:

The President's National Security Telecommunications Advisory Committee (NSTAC)'s mission is to provide the U.S. Government the best possible industry advice in these areas. For over 25 years, the NSTAC has brought together up to 30 industry chief executives from major telecommunications companies, network service providers, information technology, finance, and aerospace companies. These industry leaders provide the President with collaborative advice and expertise, as well as reviews and recommendations. The NSTAC's goal is to develop recommendations to the President to assure vital telecommunications links through any event or crisis, and to help the U.S. Government maintain a reliable, secure, and resilient national communications posture.

The Partnership for Critical Infrastructure Security (PCIS) has been actively involved in encouraging and participating in a productive public-private partnership with the Federal government over the past six years. Its focus is on improving the security and

safety of the Nation's critical infrastructures by enabling critical infrastructure sectors to work among themselves, as well as work in partnership with the Federal government. The mission of the PCIS is to coordinate cross-sector initiatives that promote public and private efforts to help ensure secure, safe, and reliable critical infrastructure services. This mission encompasses physical, cyber, and human security that rely on strong infrastructure integrity and resilience.

The Communications Sector Coordinating Council (CSCC), with its government partners, works to protect the U.S.'s communications critical infrastructure and key resources (CIKR) from harm and to ensure that the U.S.'s communications networks and systems are secure, resilient, and rapidly restored after a natural or manmade disaster. The CSCC coordinates with the other 17 critical infrastructure sectors through the Partnership for Critical Infrastructure Security (PCIS) to address cross-sector issues and interdependencies. The PCIS provides senior-level cross-sector strategy coordination through partnership with DHS and the sector-specific federal agencies or SSAs.

The National Cyber Response Coordination Group (NCRCG) is made up of 13 federal agencies and is the principal federal agency mechanism for cyber incident response. In the event of a nationally significant cyber-related incident, the NCRCG will help to coordinate the federal response, including the U.S.-Computer Emergency Readiness Team (US-CERT), law enforcement and the intelligence community.

US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local governments, and others to disseminate reasoned and actionable cyber security information to the public law enforcement and the intelligence

community. The National Cyber Alert System was created by US-CERT and DHS to help consumers and businesses protect their computers. One of US-CERT's overarching goals is to provide timely information about security topics and events.

The National Cybersecurity Center brings together federal cybersecurity organizations, by virtually connecting and in some cases, physically collocating personnel and resources to gain a better understanding of the overall cybersecurity picture of federal networks. The Center has coordinating authority and is responsible for situational awareness and reporting across the .mil, .gov and .ic domains.

NetGuard brings together the private sector with the State and local community following an incident that affects information systems and communications networks. The intent of this DHS-led initiative is to create teams of volunteers from the private sector that could provide technical assistance and resources to the affected community. The program also acts as a clearinghouse for matching the needs of the local government and businesses with available resources in a timely manner.

C. What market incentives exist for commercial communications providers, large and small, to invest in secure infrastructure? (i.e., how do we avoid externalities?)

To survive in the highly competitive marketplace, Verizon and other communications providers must be able to address cybersecurity issues that affect their networks and users. Communications providers must provide network services that are available and free from virus or worm-induced congestion. And communications providers must protect their customers and their data from attacks and losses at the hands of hackers and other bad actors. Verizon spends billions of dollars each year – recently

estimated around $17 billion – to build, maintain and protect the health of its networks.[9] As Verizon's CEO Ivan Seidenberg recently explained, "Our job is to make certain those networks are safe and reliable enough for the security of our nation – and our world – to depend on."[10]

In addition, the deployment of more advanced and intelligent broadband networks – such as Verizon's FiOS network or 4G wireless networks – would further the interests in more secure network infrastructure. New restrictions on providers' ability to offer differentiated services or to effectively manage their networks would have the opposite effect.

D. Do end-users have sufficient independent information to make good decisions between communications providers that may differ in the extent to which they implement cyber security measures?

On the consumer broadband side, Verizon provides a full complement of Internet security products and services designed to support a safe online experience for its customers and their families. In particular, Verizon provides virus protection, firewall, parental controls and anti-spyware, and makes information about each of these services available to consumers through Verizon's website. In addition, Verizon engages in a variety of proactive security activities for its broadband subscribers. Government policies that restrict network management practices or that chill continued innovation and investment in more intelligent broadband networks would make consumers' broadband services less robust and less secure.

---

[9] *See* Ivan Seidenberg, Defense Information Systems Agency (DISA) Customer Partnership Conference Keynote Address, http://newscenter.verizon.com/leadership/speeches/defense-information-systems.html.

[10] *Id.*

With respect to enterprise, government, and wholesale customers, Verizon offers a wide range of premises-based and network-based security services that specifically address network-based cybersecurity activity (e.g., managed firewall services; distributed denial-of-service mitigation services; virtual private network services that provide encrypted transport for Internet communications); professional consulting services that help Verizon's customers conduct cybersecurity risk assessments and thereafter design, architect, implement, monitor, audit, and test their networks from a security perspective; professional forensic services that provide Verizon security experts to help customers untangle a security incident, understand what was lost, and take appropriate remedial measures; and security device testing and certification services through Verizon's ICSA Labs group. Not only does Verizon provide this wide range of security-related services to its enterprise, government, and wholesale customers, Verizon security experts are available to discuss these services with Verizon customers at any point in the sales or post-sales process to help them make the most informed decisions around their investments in network and computer security.

Verizon's activities, coupled with the activities of myriad other organizations in the cybersecurity area, help inform consumer, business, and government end users as to a wide range of cybersecurity threats and what to do about them. In addition, many of these sources of independent information allow customers to compare providers' cybersecurity/internet security measures. For example, PC Magazine, Consumer Reports, CNet, and JD Power and Associates all provide objective evaluations of internet access providers.

E. How widely are cyber security best practices implemented by communications providers and what are these best practices?

Recently, the Commission took an important step with respect to cybersecurity when it re-chartered the Communications Security, Reliability, and Interoperability Council (CSRIC). The CSRIC is an advisory committee, consisting of public and private entities, that provides guidance and expertise on the nation's communications infrastructure and public safety communications. There are a wide range of security standards and best practices in the areas of network and computer security. The CSRIC could be tasked with recommending best practices and actions that the government and the communications sector can implement to ensure the security of cyberspace for economic and public safety reasons. The Commission should not mandate best practices, however, for two reasons: (a) cyber threats evolve and prescriptive practices will be overcome by evolving threats; and (b) mandates may discourage open participation and collaboration in future CSRICs.

Historical experience demonstrates the success of voluntary best practices. From 2004 through 2006, Verizon and Verizon Wireless participated on the Network Reliability and Interoperability Council (NRIC VII) subcommittee on cybersecurity. The NRIC subcommittee created a report that documented over 200 best practices related to cybersecurity. The report analyzed existing cybersecurity best practices, such as identity management, messaging security, attacks and wireless security. Verizon and Verizon Wireless recommended additions, deletions and modifications to those existing best practices and identified new best practices for the NRIC subcommittee to adopt. Verizon and Verizon Wireless have implemented a number of these best practices on a broad

scale and have found them to be effective in helping to better secure the network from physical and virtual threats.

CONCLUSION

The Commission should take the measures described above to further enhance public safety and provide better protection against cyber attacks.

Respectfully submitted,

Michael E. Glover
Of Counsel

Karen Zacharia
Mark J. Montano
VERIZON
1320 North Courthouse Road
9th Floor
Arlington, VA 22201
(703) 351-3158

John T. Scott, III
VERIZON WIRELESS
1300 I Street, N.W.
Suite 400 West
Washington, DC 20005
(202) 589-3740

Attorneys for Verizon and Verizon Wireless

November 12, 2009