

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

In the Matter of )  
 )  
Cyber Security Certification Program ) PS Docket No. 10-93  
 )  
 )  
 )  
 )  
 )  
 )

**COMMENTS OF VERIZON AND VERIZON WIRELESS**

Michael Glover  
*Of Counsel*

Karen Zacharia  
Mark J. Montano  
VERIZON  
1320 North Courthouse Road  
Ninth Floor  
Arlington, Virginia 22201  
(703) 351-3060

John T. Scott, III  
VERIZON WIRELESS  
1300 I Street N.W.  
Suite 400 West  
Washington, DC 20005

July 12, 2010

## TABLE OF CONTENTS

<b>I. Verizon Is Actively Protecting Its Networks from Cyber Attacks.</b> .....	2
<b>II. Verizon Works Closely With the Government and Others in the Larger Cybersecurity Community To Address Cyber Threats.</b> .....	5
<b>III. The Government Should Adopt a Unified Approach to Cybersecurity That Emphasizes Flexibility, Speed, and Information Sharing.</b> .....	8

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

In the Matter of )  
 )  
Cyber Security Certification Program ) PS Docket No. 10-93  
 )  
 )  
 )  
 )  
 )  
 )

**COMMENTS OF VERIZON AND VERIZON WIRELESS**

The government’s interest in cybersecurity is timely and crucial to the security of our nation. As a provider of communications services to millions of customers around the world, Verizon addresses cyber attacks daily and has developed a wide range of measures intended to help protect its network and the networks of its customers. Because this is not a fight that should be left solely to the private sector, the government has an important role in cybersecurity. However, the government should adopt a unified approach to cybersecurity and reconcile the various activities that take place today at Congress and numerous agencies. Verizon welcomes the opportunity to work with the government on a collaborative basis to shape that cybersecurity policy and better secure the nation’s networks. But this should be done in the most efficient manner possible and avoid costly duplication that would divert scarce resources from protecting the networks. As such, the Commission’s well-intentioned proposal to develop a cybersecurity certification program should not proceed unless and until integrated into a unified approach supported by the rest of the government.

## DISCUSSION

### I. Verizon Is Actively Protecting Its Networks from Cyber Attacks.

Broadband providers, including Verizon, are devoting substantial resources to protect their networks from cyber attacks even in the absence of government mandates. Given the nature of Verizon's business and the highly competitive environment in which Verizon operates, cybersecurity is vitally important to Verizon. Verizon manages thousands of voice, video, and data networks at the local, regional, national, and international level. It operates a global backbone network that carries large volumes of the Internet's traffic, one of the many thousands of independently owned and operated networks that make up today's global Internet. Verizon's data network includes more than 633,000 route miles of terrestrial and undersea cable, spanning six continents, and reaching customers in more than 2,700 cities and 150 countries. Verizon provides communications services to tens of thousands of businesses and government agencies around the globe, including 97% of Fortune 500 companies and roughly 8 million residential broadband customers here in the United States.

The nature of the Internet itself contributes to the risks faced by these customers. The Internet is not centrally controlled or managed. Rather, it is a globally distributed network-of-networks linked solely by implementation of a few common Internet protocols. It imposes virtually no barrier to any person seeking to reach a global audience. But as with many technologies, the same capabilities that make the Internet a useful tool for those with good intent can also be used by those with harmful intent. For example, the Internet allows for the rapid adoption of useful software applications that enhance users' lives, but it also allows for the dissemination of harmful viruses and

malware that destroy and steal data. The crossborder nature of the Internet magnifies its potential for good, but also complicates law enforcement.

Verizon must effectively manage these risks to compete in the highly competitive broadband marketplace. Unless Verizon's networks add value, customers will not use them. Customers who are assailed by denial of service attacks, spam, phishing, identity theft, network scanning, hacking, and other criminal activity will not be Verizon's customers for long. Rather, they will quickly move to a network that is better protected.

Verizon engages in a wide range of activities to enhance cybersecurity for itself, its customers, and other users of its network.<sup>1</sup> For example, before even deploying network assets, Verizon works closely with its vendors to help ensure that their products are able to meet Verizon's stringent security requirements. Verizon's network security group manages security on its networks using a variety of tools, security sensors, and other technologies to identify and mitigate threats on the Internet as they are emerging. Verizon takes action daily to address spam, phishing, denial-of-service, and other malicious activity that threaten to disrupt the network or its customers' use of it. Furthermore, Verizon invests in advanced threat detection and mitigation technologies and other research and development to deal with emerging and future threats.

In addition to protecting Verizon's core networks, it is critically important that Verizon's customers adequately secure their own networks and data. Verizon offers customers a wide range of cybersecurity services, including managed firewall, intrusion detection, intrusion prevention, and encrypted virtual private networking. Verizon's

---

<sup>1</sup> The descriptions herein are at a relatively high level to avoid providing wrongdoers with a roadmap that would allow them to circumvent Verizon's protective measures.

security-certified data centers offer enhanced security features for customer systems and data, and Verizon offers professional services pertaining to security consulting, network analysis, incident response, and computer forensics. For federal government customers, Verizon's Government Network Operations and Security Center provides a single point of contact to obtain products and services to meet network operations requirements, including those related to security matters. For residential broadband customers, Verizon offers parental controls, anti-spam features, and other security software to assist them in securing their computers.

Verizon applies the same practices to protect its own corporate systems. Verizon inventories its enterprise, network-connected systems and assigns them a criticality score based on the sensitivity of the data they contain. Verizon then periodically scans the systems to identify security vulnerabilities. These results are correlated to threats and system value, and the results are automatically displayed on Verizon's internal security event management systems. This real-time threat and vulnerability information about Verizon's systems has proved invaluable to identifying affected systems and establishing priorities for remediation. Internal groups compete against each other to see who can consistently maintain the cleanest scorecard.

Finally, Verizon's cybersecurity efforts redound to the benefit of all Internet users, whether they are customers or not. A healthy Internet backbone is critical to users who connect through any ISP. Moreover, Verizon spends thousands of hours each year analyzing data collected from its involvement in cybersecurity events and publishes for free an annual data breach investigation report (DBIR). This report uses an information-sharing framework called VERIS, which Verizon has also made available for

free. The report provides valuable advice and guidance for enterprise and government customers on tangible, effective steps they can take to better secure their networks today.

## **II. Verizon Works Closely With the Government and Others in the Larger Cybersecurity Community To Address Cyber Threats.**

Verizon is a leader in the larger cybersecurity community, where it has worked closely with the government and other companies within the communications sector during recent, significant cyber attacks. In particular, Verizon has relationships with several organizations that were created in response to earlier threats to the nation's critical infrastructure. Some of the organizations that Verizon has a leadership role in or is a significant participant in include the President's National Security Telecommunications Advisory Committee (NSTAC), the National Coordination Center for Telecommunications (NCC), the Communications Sector Coordinating Council (C-SCC), the National Security Information Exchange (NSIE), and the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC). Verizon has long cooperated with these entities and others to prepare for emergencies, to deliver critical services when emergencies and disasters occur, and to assist law enforcement, to the extent authorized by law.

These pre-existing relationships, combined with flexibility, speed, and independence, are essential to Verizon's ability to prepare for and react to significant threats to its networks. Verizon's networks and its customers' networks are frequently targeted by individuals, groups, and organizations that intend to do harm. These attacks are constantly changing and evolving as criminals and hackers develop new techniques to evade the latest defenses. Once launched, these assaults can escalate with astonishing speed. Distributed virtual computer networks known as botnets can flood victims with

vast amounts of traffic, send millions of spam messages to ensnare new victims, and serve as a virtual hosting network for illicit commercial activity.

In recent years, Verizon has faced many cyberspace challenges as the four examples below demonstrate. In each of these cases, Verizon has worked with other parties (i.e., providers, companies, the government, and others) to quickly address the issue at hand. And these examples make clear the need for network providers to continue to have the flexibility, speed, and independence to resolve future cybersecurity problems as they have in the past.

1. Several years ago, a major financial services institution faced a significant distributed denial of service attack that effectively disabled its ability to handle online transactions via the Internet. Verizon worked closely with another large Internet backbone provider to quickly bring the attack under control and to help restore stability to the customer's network. Verizon would not have been able to address the issue at hand as quickly and successfully if it had been required to brief and share information with outside parties on a real-time basis or wait for feedback on, or concurrence with, its plan of action.

2. The SQL-Slammer worm was launched on January 25, 2003 at approximately 12:30 a.m. EST, and began rapidly spreading across the Internet. At that time, this worm was the fastest spreading computer worm in history, doubling in size every 8.5 seconds. Within three minutes, the worm achieved its full potential – with more than 55 million computers being scanned per second. The Slammer worm infected more than 90% percent of vulnerable hosts within 10 minutes. This rapid spread caused significant disruption to financial, transportation, and government institutions. Success in

stopping the Slammer worm was predicated on the ability of network operators to take fast and decisive action without extraneous briefings, consultations, or declarations.

3. The recent Conficker worm experience illustrates the importance of flexibility in responding to an attack and demonstrates how existing information sharing activities can be effective. Conficker has spawned one of the most successful and robust criminal botnets in history. It was first released on November 21, 2008, just weeks after publicity about a critical software vulnerability affecting operating systems used in a large portion of the computing infrastructure on the Internet. In response to this threat, an international working group – the Conficker Working Group – was formed, consisting of thirty named members and many more partners and contributors around the world, including industry (including Verizon), governments, and educational institutions. The Conficker Working Group’s efforts have largely prevented the monetization of this criminal botnet and helped to hamper its spread at key points in its evolution. The Conficker Working Group may have bought additional time for more sites to patch the vulnerability and implement additional security measures.

After almost two years, this botnet remains a threat to the world’s networks, and those responsible for releasing and controlling it are still at large. Because the data and expertise needed to counter this type of cyber threat are distributed globally among companies, universities, and governments, it is important that the lines of communication remain open.

4. The Rinbot incident in 2006-2007 highlights the damage that can be caused when an average miscreant armed with powerful hacking tools that are widely and cheaply available on the Internet “black market” takes aim at just a few critical

vulnerabilities in unpatched systems connected to the Internet. Security sensors deployed in Verizon's Internet backbone network alerted Verizon's network security teams to an emerging outbreak. The teams disseminated this information quickly within the company, to customers, to the impacted vendor, and to numerous established cross-industry groups. Verizon's information helped prioritize the identification, mitigation, and ultimate takedown of the Rinbot botnet. Although the aggressive nature of this virus led to the complete shutdown of a regional hospital network in Canada and several enterprise networks in the United States, the quick action by Verizon and others helped prevent far greater harm.

In sum, Verizon and others in the industry are focusing on efforts to safeguard consumers and our country's networks. These examples illustrate that public and private sector response and remediation activities and information sharing exist today in ways that are highly advanced and effective, and that speed and flexibility are essential for combating such cyber threats. Even without government mandated practices or oversight, private sector operators are – and have been for years – moving “full speed ahead” to expand their tools, expertise, and capabilities necessary to identify threats, address them, and preserve providers' ability to serve their customers.

### **III. The Government Should Adopt a Unified Approach to Cybersecurity That Emphasizes Flexibility, Speed, and Information Sharing.**

Due to existing cybersecurity mechanisms already in place, the government must tread carefully so that any new regulation does not disturb the current systems or divert network operators' resources from security enhancements. Yet that does not mean that the government has no role in enhancing cybersecurity. In fact, there are proactive steps

the government can take because the government is uniquely positioned to do things the private sector simply cannot.

Government efforts should be focused on the following key goals and objectives:

1. *Centralize and clarify government roles and responsibilities.* The government needs to speak with one voice when setting national priorities and agendas. There should be consistency in the government's views and in the security of its infrastructure. The government should secure its own networks and systems by using its purchasing power to obtain best-of-breed security features, thus protecting some of our nation's most critical information assets and facilitating the development of new security offerings.

2. *Avoid duplication of cybersecurity initiatives.* Given the wide-spread level of concern across all government sectors on cybersecurity issues, it is not surprising that many different proposals exist for how to best address it. Unnecessarily duplicative or inconsistent initiatives threaten to drain scarce resources and divert industry from substantive cybersecurity activity.

For example, within the past four months, Senators Rockefeller and Lieberman have each introduced comprehensive cybersecurity legislation – both of which have been passed out of their committees (Commerce, Science, and Transportation and Homeland Security and Government Affairs, respectively) – that would establish a formal government role and place certain requirements on providers of critical infrastructure. At the same time, Senator Bond, who sits on the Intelligence Committee, has prepared his own draft of cybersecurity legislation addressing many of the same topics as his

colleagues. Likewise, members of the House have been involved in drafting various cybersecurity legislation.

In addition to the legislative branch, the Department of Homeland Security and the National Security Agency have long been responsible for developing defenses to cyber attacks. The White House's Comprehensive National Cybersecurity Initiative, which was established in 2008, has set out a number of cybersecurity initiatives, many of which closely track the goals and objectives suggested here.<sup>2</sup>

Moreover, a number of departments and agencies that traditionally have been less involved in cybersecurity issues have recently taken on cybersecurity initiatives. Just two weeks ago, the National Institute of Standards and Technology (NIST), the National Telecommunications and Information Administration (NTIA), and the International Trade Administration (ITA), on behalf of the U.S. Department of Commerce, announced a public meeting to discuss "emerging techniques used in successful cybersecurity strategies, and the relative roles of the private and public sectors with respect to improving cybersecurity in the commercial arena."<sup>3</sup> NIST has also been actively examining cybersecurity practices relating to Smart Grids.<sup>4, 5</sup>

If concrete steps are taken by one government entity without harmonizing its cybersecurity policy with the rest of the government, that would introduce substantial

---

<sup>2</sup> See <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative> (last visited July 9, 2010).

<sup>3</sup> Department of Commerce, *et al.*, Notice of Public Meeting, *Cybersecurity and Innovation in the Information Economy*, 75 FR 36633-634 (June 28, 2010).

<sup>4</sup> See National Institute of Standards and Technology, Request for Comments, *Draft NIST Interagency Report (NISTIR) 7628, Smart Grid Cyber Security Strategy and Requirements*, 74 FR 52183 (Oct. 9, 2009).

<sup>5</sup> To the extent possible, Verizon participates in these government activities relating to cybersecurity. Last month, for example, Verizon's Chief Network Security Officer testified before the Homeland Security and Government Affairs Committee.

inefficiencies. Accordingly, the Commission's proposed voluntary cybersecurity certification program should not move forward until a unified approach to cybersecurity is developed.

3. *Promote enhanced security for private sector infrastructure while maximizing private sector flexibility and preserving speed of response.* Because there may be those in the private sector that are slow in adopting appropriate cybersecurity practices, government should provide incentives for them to do so. This would benefit all networks that connect with those networks. However, given the wide range of networks and technologies, as well as the rapid pace with which cyber threats are ever-evolving, the government should not mandate a single approach. Network providers must retain the freedom to implement any measures to secure their infrastructure and critical systems, including the freedom to take rapid, decisive action without being subject to regulatory second-guessing.

4. *Encourage a public-private partnership.* The most effective approach to cybersecurity is a public-private partnership where government provides assistance and expertise to the private sector, coupled with incentives like confidentiality and liability protection to encourage the private sector to implement desired activities and with freedom to take decisive actions. Unfunded regulatory mandates and command-and-control type governance structures must be avoided.

5. *Drive diplomatic efforts to reduce the number of countries that are havens for cyber criminals.* International diplomacy is one of the key objectives of any national strategy to increase the security of cyberspace. The government should work with other

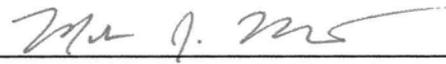
governments to persuade regimes that are havens for cyber criminals to take a firmer stand in support of global Internet security.

6. *Remove outmoded legal barriers to appropriate information-sharing.* A number of outdated laws, including the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, present barriers to the collection, use, and sharing of information by network operators and their customers, and the government. This patchwork of laws needs to be updated so that there is a coherent legal framework that takes into account the current state of technology and strikes the appropriate balance between privacy and the need for information sharing among the government and the private sector.

## **CONCLUSION**

Cybersecurity is an important topic on which both the government and private entities should be focused. The government should adopt a single approach to cybersecurity, emphasizing private-sector flexibility, speed, and information sharing, before the Commission proceeds with any specific cybersecurity programs. Verizon welcomes the opportunity to work with the government on a collaborative basis to better secure the nation's networks.

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*

July 12, 2010