TESTIMONY OF
SARA C. SANTARELLI
VERIZON COMMUNICATIONS

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

"PROTECTING CYBERSPACE AS A NATIONAL ASSET: COMPREHENSIVE LEGISLATION FOR THE 21ST CENTURY"

JUNE 15, 2010

Mr. Chairman, Ranking Member Collins, and members of the Committee, thank you for this opportunity to discuss the important topic of cyber security. My name is Sara Santarelli and as Verizon's Chief Network Security Officer my primary responsibility is to ensure the integrity of Verizon's network systems, including risk management, threat detection, and incident response.

The Committee's interest in cyber security 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 our network and the networks of our customers. But this is not a fight that should be left solely to the private sector—there is a very important role for government in securing cyberspace and we applaud the Committee's efforts to help bring clarity and definition to that role.

The legislation you have proposed represents a positive step forward in building a stronger bond between the public and private sectors with respect to cyber security. While we may not agree with some of the finer points in the bill and look forward to working with your staff to iron out those differences, we feel that the majority of the legislation supports the common goal of creating a much safer online environment for our customers and for the nation. We appreciate the difficulty you face in crafting legislation that is constructive and useful for increasing our nation's security in cyberspace, while also not placing an undue burden on private companies, large and small, that are struggling in the current economic downturn.

My testimony gives you a brief background of what cyberspace looks like from our point of view and provides several examples of actions we've taken over the past few years to address and mitigate online threats. It identifies how we believe a strong partnership between the private companies that own and operate the networks that make up cyberspace can be established with government agencies that are responsible for providing for the security of our nation against all threats, including those in the virtual world.

Verizon manages thousands of voice, video, and data networks at the local, regional, national, and international level. Ours is 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. We provide communications services to tens of thousands of businesses and government agencies around the globe, including 97 percent of Fortune 500 companies and roughly 10 million residential broadband customers here in the United States.

Given the nature of our business, cyber security is vitally important to us. 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. The number of people connected to the Internet is estimated by some to exceed 1 billion, and not all of them have good intentions. 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 that destroy and steal data. It allows for consumers and companies to interact more efficiently with one another, but it also could be used to attack and disrupt commercial transactions. The cross-border nature of the Internet magnifies its potential for good but also complicates law enforcement.

This is the reality Verizon deals with every day. As a result, Verizon engages in a wide range of activities to enhance cyber security for ourselves, our customers, and other users of our network. These activities take place at many different layers within our organization. For example, before even deploying our network, we work closely with our vendors to help ensure that their products are able to meet our security requirements. Our network security group manages security on our networks using a variety of tools, security sensors, and other technologies to identify and mitigate threats on the Internet as they are emerging. We take action daily to address spam, phishing, denial-of-service and other malicious activity that threatens to disrupt our network or our customers' use of it. We invest in advanced threat detection and mitigation technologies. We also make strategic R&D investments to develop new technologies that deal with emerging and future threats.

In addition to addressing cyber security issues in our network core, we offer a wide range of services to help customers secure their networks and data. Services such as managed firewall, intrusion detection, intrusion prevention, and encrypted virtual private networking help customers keep their networks safe. Verizon's Government Network Operations and Security Center provides federal agencies with a single point of contact to obtain products and services to meet network operations requirements and related security matters, putting both network and security operations under one umbrella. Our security-certified data centers offer enhanced security features for customer systems and data. For residential broadband customers we offer parental controls, anti-spam features, and other security software to assist them in securing their computers.

Going beyond our network services, we offer a wide range of professional services to include security consulting, network analysis, incident response, and computer forensics. Our professional security engineers hold over sixty different certifications and federal clearances, and are available 24/7 around the world to assist customers in responding to breaking cyber security incidents.

When it comes to the security of critical networks and systems, we practice what we preach. Within our own enterprise, network-connected systems are inventoried and assigned a criticality score based on the sensitivity of the data they contain. They are then scanned periodically to identify security vulnerabilities. The results of the scanning activity are correlated to threats and system value, and the results are automatically displayed in real time on our internal system security dashboard. This real-time threat and vulnerability information about our own corporate systems has proved invaluable to our internal business leaders in helping them identify affected systems and establish priorities for remediation. Internal groups actually compete against each other to see who can consistently maintain the cleanest scorecard!

Our backbone security activities redound to the benefit of all of our users at no charge. We spend thousands of hours each year analyzing data collected from our involvement in cyber security events which, after rigorous scrubbing to remove any attribution, we publish, free of charge, in our annual data breach investigation report (DBIR). This report, which uses a Verizon-developed information-sharing framework called VERIS that we have also published as an open-source initiative, provides valuable advice and guidance for enterprise and government customers on tangible, effective steps they can take to better secure their networks today. The bottom line for Verizon is that unless our networks add value, our customers won't use them. Customers who are assailed by denial of service attacks, spam, phishing, identity theft, network scanning, hacking, and other criminal activity won't be customers of ours for long. They will quickly move to a network that is better protected.

Finally, we view ourselves as being a leader in the larger cyber security community. Verizon and other companies within the communications sector have a long history of cooperation in emergency preparedness and assisting law enforcement, to the extent authorized by law. This history distinguishes the sector from most other critical sectors identified in the National Infrastructure Protection Plan and is a reflection of our relationship with the federal government and the public policy community. The sector personifies cooperation and trusted relationships, which has resulted in the delivery of critical services when emergencies and disasters occur. This strong bond between the private and public sectors exists today in large part because of 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).

Security events are a constant reminder that our networks and our customers' networks are under a steady assault from individuals, groups, and organizations that intend to do harm. And it is important to note that these assaults are constantly changing and evolving as criminals and hackers develop new techniques to get around the latest defenses. Once launched, these assaults can escalate with astonishing speed. Improvements in computer processing power, memory, and bandwidth not only help support new lawful applications like VoIP and streaming video, but they also enable hackers to wield tremendous weapons in cyber space. 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. Government regulation of private sector network security activities must not diminish the flexibility, speed, and independence that network providers find essential in waging war on cyber crime.

In recent years, we have faced many cyberspace challenges as the four examples that follow demonstrate. In each of these cases, we have worked with other parties (providers, companies, the government, and others) to quickly address the issue at hand. Any new requirements must continue to afford us the flexibility and speed to continue resolving problems as we have in the past.

- Several years ago a major financial services institution was under a significant distributed denial of service attack that effectively disabled its ability to handle online transactions via the Internet. We 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. We would not have been able to address the issue at hand as quickly and successfully if we had been required to brief and share information with outside parties on a real-time basis or wait for feedback on, or concurrence with, our plan of action.

- 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. The scanning technique used by the Slammer worm was so aggressive that it quickly interfered with its own growth. Within three minutes the worm achieved its full potential (with more than 55 million computers being scanned per second), at which point its growth rate slowed. Slammer 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 to take fast and decisive action without extraneous briefings, consultations, or declarations.

- The recent Conficker worm experience illustrates how important it is to maintain flexibility in any cyber regulatory regime. 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 (CWG)—was formed. It consists of thirty named members and many more partners and contributors around the world, including Verizon. This global partnership involved industry, governments, and educational institutions. Its efforts have largely prevented the monetization of this criminal botnet and hampered its spread at key points in its evolution. It bought additional time for more sites to fix vulnerabilities by implementing additional security controls. This botnet remains a clear threat to the world's networks and those responsible for releasing and controlling it are still at large after almost two years. Conficker is a good example of a complex and rapidly evolving threat for which existing information sharing activities have proved effective. The data and expertise needed to counter cyber threats such as this are distributed globally among companies, universities, and governments. When those groups work together, the result is greater than the mere sum of the parts. It is imperative that any government-directed information sharing mechanism be nimble and flexible enough to accommodate any and all comers, and not otherwise place restrictions or requirements on the free flow of information about the Internet.

- 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 our network security teams to an emerging outbreak. We 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, we believe that quick action by Verizon and others helped prevent far greater harm.

Headlines often make it appear that the Internet is so vulnerable and open to attack that nothing can be done or is being done to safeguard consumers and our country. But what these events illustrate is 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 information sharing and 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.

That's not to say there is not a role for government—there is. The government is uniquely positioned to do things the private sector simply can't. For example, the government has the power to:

- Share unique and valuable information resources that it possesses which might aid private-sector cyber security efforts;
- Work with industry to define mutually-agreeable plans for addressing potential incident scenarios before such incidents occur;
- Incent those who are slow in adopting cyber security best practices to improve their security posture, thus reducing the negative externalities that exist from the under-investment by some in adequate network security;
- Secure its own networks and systems, thus protecting some of our nation's most critical information assets;
- Facilitate the development of new security offerings by requiring best-of-breed security features in the products it purchases;
- Provide valuable incentives for desirable private action, such as limitations on liability for collateral damage flowing from otherwise desirable network security behavior;
- Clear away outdated legal barriers that impair some of today's cybersecurity activities; and
- Work with other governments, to persuade regimes that are havens for cyber criminals to take a firmer stand in support of global Internet security.

With this in mind, we believe government efforts should be focused on the following key goals and objectives, most of which are addressed in the proposed legislation:

- Centralize and clarify government roles and responsibilities. The government needs to speak with one voice when setting national priorities and agendas. Proposals in this bill such as the Office of Cyberspace Policy and the National Center for Cybersecurity and Communications, for example, could streamline interactions and ensure consistency in the government's view and in the security of its own infrastructure.

- Avoid duplication of cyber security initiatives. Given the wide-spread level of concern across all government sectors on cyber security 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 us from substantive cybersecurity activity. This bill takes several steps towards achieving the goal of reduced duplication of initiatives, and we appreciate the effort that this will take.

- Promote enhanced security for private sector infrastructure while maximizing private sector flexibility and preserving speed of response. Clearly, there will always be those who are slow in adopting best practices in the area of cyber security. It is appropriate for government to provide strong incentives for those enterprises to enhance their level of security. Given the wide range of networks and technologies, as well as the rapid pace with which cyber threats are ever-evolving, it is imperative that we do not lock ourselves into a single regulated approach. Owners/operators of critical infrastructure must retain the freedom to implement any and all measures available to them to secure their infrastructure and critical systems. With respect to speed-of-response—speed that is often measured in seconds, not hours or days—it is essential that providers have the freedom to take decisive action to protect their critical cyber resources without being subject to regulatory second-guessing. Unfunded regulatory mandates and command-and-control type governance structures must be avoided. The most effective approach, which appears to be the direction that this bill is taking, 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.

- Drive diplomatic efforts to reduce the number of countries that are havens for cyber criminals. While this legislation does not directly address international diplomacy, it does recognize that it is one of the key objectives of any national strategy to increase the security of cyberspace.

- Remove outmoded legal barriers to appropriate information-sharing. A number of outdated laws present barriers to the collection, use, and sharing of information by network operators and their customers, and the government. We urge you to update this patchwork of laws and provide 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 government and the private sector.

We look forward to working with you and your staff on further refining these mechanisms to ensure that network service providers and other private sector actors retain the freedom to act quickly as they see fit to address these ever-evolving and rapidly spreading threats to our networks, our economy, and our way of life.

Mr. Chairman and members of the Committee, I again thank you for the opportunity to appear before the Committee to discuss the important topic of cyber security and the challenges of securing critical infrastructure information systems. I look forward to answering any questions you may have.