

**Testimony of
James Arden Barnett, Jr.
Rear Admiral, USN (Retired)
Chief, Public Safety and Homeland Security Bureau
Federal Communications Commission**

**Before the
Subcommittee on Communications, Technology and the Internet
Committee on Energy and Commerce
U.S. House of Representatives**

**Hearing on “Cybersecurity: Threats to Communications Networks and
Public-Sector Responses”**

March 28, 2012

Good morning, Chairman Walden, Ranking Member Eshoo, and distinguished members of the Subcommittee. Thank you for the opportunity to testify on the important topic of cybersecurity threats to communications networks. The Federal Communications Commission has been working with a broad cross-section of the broadband economy; world-class engineers who helped invent and develop the Internet and who understand the latest technologies and trends; award-winning academics; and dedicated federal partners from across government to address the threat posed by cyber attacks.

As you are all aware, cyber attacks present a critical threat to our economic future. More than \$8 trillion dollars flow over these networks each year and that amount is growing. Approximately 150 million Americans shop or bank online.¹ And more than 1 million entrepreneurs rely on these networks for the life blood of their businesses.

Beyond commerce, these networks are driving breakthroughs in health care, education, energy, manufacturing, public safety, and other sectors of the economy, as well as providing a forum for free speech and expression of which our founding fathers would be proud. Simply put these networks have transformed the way we connect and communicate with one another and they have transformed every sector of our economy and the world economy.

The benefits of this transformation however do not come without security risks for consumers, businesses, and government.

¹ See <http://www.emarketer.com/blog/index.php/tag/how-many-people-shop-online/>

For example, in April 2011, a massive cyber-attack on Sony's PlayStation Network and Qriocity services led to the compromise of 77 million user accounts. In hacking the Japanese company's database, thieves made off with personally identifiable user information, including dates of birth, e-mail and home addresses and login credentials.² Millions of Americans are unaware that their home or office computers have been infected and are being controlled remotely by cyber criminals, so called botnets, that send spam or secretly attack the websites of businesses, not-for-profits, and government agencies. Citigroup is one of several high-profile companies that suffered a cyber-attack. In June of 2011, the bank reported that 210,000 of its card holders had their personal data compromised by hackers. The stolen information included names, account numbers and e-mail addresses.³

In May, Fidelity National Information Services reported that profits experienced a \$13 million loss due to "unauthorized activities." A group of criminals hacked the company's network and gained access to its central database where card balances are kept. The criminals then obtained 22 legitimate prepaid cards, and made copies that were shipped to conspirators in Greece, Russia, Spain, Sweden, Ukraine and the United Kingdom. The crooks were able to increase the balances of the cards, making it possible for their worldwide criminal partners to withdraw cash from dozens of ATMs during a 24-hour period.⁴

The Ponemon Institute found that the median annualized cost of cyber crime for the 50 organizations in their study was \$5.9 million, with the range being \$1.5 million to \$36.5 million.⁵ According to a Symantec survey, three-quarters of small and medium businesses report being affected by cyber attacks.⁶

No one would tolerate this level of criminality, thievery, vandalism, or invasion of property if it was done in the physical world, and we can no longer afford to tolerate it in cyberspace.

Private Industry's Response

Luckily, the United States has the resources to respond to these threats. The approximately 40,000 autonomous systems or networks on which the Internet is built are largely commercial or privately owned, and connected on the basis of trust, a basis that is increasingly vulnerable.. The

² See <http://www.crn.com/slide-shows/security/232300672/10-biggest-security-breaches-of-2011.htm?pgno=11>

³ See <http://www.crn.com/slide-shows/security/232300672/10-biggest-security-breaches-of-2011.htm?pgno=9>

⁴ See <http://www.crn.com/slide-shows/security/232300672/10-biggest-security-breaches-of-2011.htm?pgno=10>

⁵ See http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

⁶ See

http://www.symantec.com/content/en/us/about/media/pdfs/SMB_ProtectionSurvey_2010.pdf?om_ext_cid=biz_soc_med_twitter_2010Jun_worldwide_SMB at 3.

commercial communications providers are therefore the first line of defense against cyber threats and always will be.

I have had the opportunity to visit some of their operations centers, and on a minute-by-minute basis, around the clock, these providers ably and vigorously defend their networks from constant attacks. I am very impressed with the level of expertise and dedication that these commercial providers exert to protect against these cyber attacks. Earlier this month, on March 7, this subcommittee heard from cybersecurity experts in the communications industry about how hard they are working against those threats and those attacks.

Yet, if their efforts alone were sufficient to thwart cyber threats, we would not be here today. To be successful in battling cyber threats, we must work together, collectively, private industry and the public sector.

So your line of inquiry on the proper and effective roles of government and its agencies is salient.

Principles of Government Action in Cybersecurity

In pursuing the proper roles of government in cybersecurity, we must observe some key principles:

1. We must ensure that the broadband economy remains an engine of innovation and growth, increasingly available to and used by Americans.
2. Sacrificing privacy or Internet openness for security is a false choice. We must insist on having all three, and we strongly believe that this is achievable.
3. We must preserve the multi-stakeholder model to tackle Internet issues like cybersecurity. Stakeholders across the ecosystem will need to work together and develop practical solutions to secure our networks.
4. We should seek smart, practical, voluntary solutions through cooperative efforts to achieve cybersecurity, whenever it is possible and effective.
5. Federal partners must work closely together in a whole-of-government approach. We must bring all our talent and efforts to bear and cannot afford to leave talent on the sidelines or pursue uncoordinated actions.

I will return to these principles later in my testimony, but with them in mind, I will turn to the FCC's role and actions in cybersecurity.

The FCC's Role and Actions in Cybersecurity

The FCC was established by Congress for the purpose of national defense and to promote the safety of life and property through the use of wire and radio communications. As the nation's expert agency on communications, we have always been concerned with the security and reliability of networks. The FCC has a long history of working on network reliability and security with the companies that operate the core of the Internet. In the spirit of seeking non-regulatory answers first, we have a longstanding practice of working collaboratively with

industry, federal partners, public safety, and others to enhance network reliability and security. We have had success as a convener and facilitator of the communications industry. As long ago as 2001, the FCC's industry-based advisory committee, the Network Reliability and Interoperability Council (NRIC) delivered the first set of cybersecurity best practices anywhere in the federal government.

After I arrived at the FCC in 2009, I proposed the reorganization of one of our Public Safety and Homeland Security Bureau's divisions into the Cybersecurity and Communications Reliability Division (with the approval of Congress) and continued to add cybersecurity and communications experts to augment our capability. This division helps coordinate the work of our current federal advisory committee, which succeeded the NRIC, the Communications Security, Reliability and Interoperability Council (CSRIC)

The CSRIC is now made up of over 50 industry leaders from the private sector, engineers, and the federal government, including cyber experts from DHS and NIST and a veritable all-star cast of Internet pioneers and world class cybersecurity experts.

In March 2011, Chairman Genachowski tasked the CSRIC with developing best practices to help address major Internet security vulnerabilities. The Chairman identified three areas where action is required to better protect commercial communications networks:

1. Securing the Domain Name System (DNS) to prevent spoofing and DNS cache poisoning (DNS is like the plain language telephone book for the World Wide Web to help you find where you want to go);
2. Improving the security of Border Gateway Protocols to prevent Internet route hijacking; and
3. Defeating botnets which cause distributed denial of service attacks and pilfer private information and money.

I am pleased to report that last week the CSRIC approved voluntary, industry-based recommendations addressing all three critical problems. Moreover, these recommendations are not simply a set of reports that will adorn bookshelves. Numerous ISPs, including Comcast, Verizon, AT&T, Time Warner, Sprint, Cox, T-Mobile, Frontier and Century Link have already pledged to implement the CSRIC recommendations as they apply to their respective networks and infrastructure. This means that these new cybersecurity measures will soon be protecting a significant majority of American Internet users, and we hope more ISPs will adopt these measures.

I would like to briefly describe the three network threats and vulnerabilities on which we have focused.

First, CSRIC recommended that ISPs adopt a voluntary Code of Conduct to provide a critical baseline framework of security to all Internet users to mitigate the botnet threat, which we refer to as the Anti-Bot Code. The Anti-Bot Code encourages ISPs to participate in activities in support of:

1. End-user education to prevent bot infections;
2. Detection of bots;
3. Notification of potential bot infections;
4. Remediation of bots; and
5. Collaboration and sharing of information from participating in the Code.

Of course, ISPs can and must do this in a way that does not compromise consumers' privacy. In fact, respect for privacy is a core implementation principle of the Anti-Bot Code. As such, all ISPs who volunteer to participate in the Code must agree to adhere to applicable privacy laws affecting the execution of their bot and botnet education, detection, notification, remediation, and collaboration activities. By doing so, these voluntary actions help protect the privacy of American consumers and businesses from those who would seek to steal identities, money, and property.

Industry leaders Comcast, CenturyLink and others have already implemented these measures, and as I mentioned, many other ISPs representing millions of American users signed on last week. This will not end botnets, but when fully implemented, this will make it significantly harder for bad actors to operate botnets.

The second major security challenge examined by the CSRIC is Internet route hijacking.

The autonomous networks upon which the Internet is built rely on an implicit trust that is the Internet's greatest strength, but can also be a major weakness. The protocol that enables seamless connectivity among these networks, known as Border Gateway Protocol or BGP, does not have built-in mechanisms to protect against cyber attacks. This makes it possible for bad actors to misdirect Internet traffic meant for one destination through the hands of another network.

During the time the traffic is diverted, the network through which it has been diverted can "eavesdrop" on the information passing through, stealing or changing the information before it arrives at its intended destination. Internet route hijacking can endanger valuable intellectual property, other personal property, and jeopardize our National security. In 2010, traffic to 15 percent of the world's Internet destinations was diverted through Chinese servers for approximately 18 minutes.⁷ According to numerous media reports, in 2008, traffic intended for YouTube was misrouted for about two hours due to the actions of a Pakistani Internet service provider.⁸ Misrouted traffic, whether intentional or accidental, is clearly unacceptable.

The CSRIC recommended ISPs develop a path toward the implementation of secure routing protocols and best practices to minimize the likelihood and impact of BGP exploits. In particular, it recommended:

⁷ <http://www.reuters.com/article/2010/11/19/us-china-internet-idUSTRE6AI1DK20101119>

⁸ Pakistan's YouTube Blockage Caused Outage, John Ribeiro, February 25, 2008,

<http://abcnews.go.com/Technology/PCWorld/story?id=4339294>

1. The establishment of a touchstone of ground truth, in essence, a secure, authoritative database of Internet address blocks to be used and checked by ISPs. This would be an Internet registry established by industry, not government and in fact, the American Registry of Internet Numbers (ARIN) has already volunteered to establish the registry. This is appropriate, since ARIN actually assigns IP address blocks to ISPs now;
2. The registration and maintenance of ISP address blocks in the authoritative registry; and
3. The phased deployment of techniques that detect and prevent route hijacking by checking routes against the registry. Each network would still retain the local autonomy to decide how to store, disseminate, and utilize the certified number resources information and how to route.

CSRIC also recommended better metrics and continuous monitoring to quantify the frequency and scope of routing system security incidents and to evaluate the effectiveness of proposed security improvements, particularly those related to inter-domain routing on the Internet. More work will be needed to completely secure Internet routing through a secure BGP, and some of those standards and equipment are a few years off. However, the benefits of ISPs taking these steps now to help eliminate misrouted traffic will be momentous.

Our third area of action is the Domain Name System (DNS). DNS can be thought of as the telephone book for the Internet; DNS servers are filled with identifying information for web sites, which is used to direct Internet users to websites they want to visit. The Domain Name System provides a simple and convenient way to associate and translate easily remembered names, known as domain names (for example, www.fcc.gov), to numerical IP addresses (for example, 201.96.10.10) that are used to find Internet sites.

Domain name fraud occurs when bad actors change the identifying information, so that an unsuspecting Internet user attempting to go to one website can be misdirected to another website, oftentimes a fraudulent one. The fake website may be designed to look exactly like the real one so that the user can be tricked into providing their financial and personal information.

For instance, in 2009 the customers of one of Brazil's biggest banks were the victims of DNS fraud. They found themselves on a fake website that looked exactly like the bank's real one. Customers' user names and passwords were stolen for four hours until the crime was discovered.⁹

A report by Gartner found 3.6 million Americans getting redirected to bogus websites in a single year, costing them \$3.2 billion.¹⁰

The good news is that the Internet Engineering Task Force (IETF), an organization that develops and promotes Internet standards, has developed a solution to the vulnerabilities in the Domain Name System, Domain Name System Security Extensions or DNSSEC. The extensions are an

⁹ <http://cyberinsecure.com/cache-poisoning-attack-sends-top-brazilian-bank-users-to-scam-sites/>

¹⁰ <http://www.gartner.com/it/page.jsp?id=565125>

add-on to the DNS protocol and are being used by several large ISPs and government agencies.

Since the original design of DNSSEC, measures have been taken to ensure that it functions in a way that is consistent with privacy laws. As such, DNSSEC was designed with privacy in mind and it can and must be implemented in a way that protects individual privacy. The CSRIC endorsed ISPs embarking on DNSSEC implementation, and Chairman Genachowski called for industry-wide adoption of the standard to help prevent unsuspecting Internet users being sent to fraudulent websites.

These three initiatives have been developed consistent with the principles that I stated earlier. They have been developed using a multi-stakeholder, voluntary approach. These initiatives are in keeping with Organization for Economic Cooperation and Development's principles for Internet policymaking, which emphasize the importance of multi-stakeholder cooperation to promote network security, and were endorsed by the United States and 34 other countries.¹¹ They are non-regulatory, industry-based and have been worked on in cooperation with our federal partners. These initiatives fit under the aegis of broader cybersecurity efforts being led by the Department of Commerce, the National Institute of Standards and Technology (NIST) and the Department of Homeland Security. They are common travelers with the National Strategy for Trusted Identities in Cyberspace (NSTIC). They stand as an example to the world of how to promote cybersecurity while preserving the core characteristics of the Internet that have fueled the broadband economy's growth and success.

CSRIC's work will be ongoing because bad actors will continue to try to innovate around our defenses and measures. We must out-innovate them.

In closing, I am proud of the actions that have been taken just last week on the Botnet Code of Conduct and implementation practices for securing Internet routing and the Domain Name System. The FCC will remain focused on cybersecurity threats to communications networks. We will continue to work with a wide range of stakeholders, including industry and federal partners on voluntary, industry-based solutions. We will carefully guard the reliability and security of all communications networks. Thank you.

¹¹ White House Technology website, <http://www.whitehouse.gov/issues/technology#id-1>