Military Cyber Security Conference
Holiday Inn Rosslyn
Arlington, VA

March 7, 2012, 2:50pm

Keynote Presentation:
Exploring the FCC's Role in
Communications Network Security

James Arden Barnett, Jr., Rear Admiral (Ret.)
Chief, Public Safety & Homeland Security Bureau
Federal Communications Commission

Slide 2

Good afternoon! Thank you [Steve Haynes and thanks] for the opportunity and your time to discuss the role of the Federal Communications Commission in communications network security and cybersecurity and how it may impact the integrity of the Domain Name System, Internet route hijacking, and finally botnets.

Slide 3

For context, let me tell you a little bit about the FCC and about the Public Safety & Homeland Security Bureau, of which I am privileged to be the Chief. The FCC is an independent agency, usually consisting of 4 commissioners, two from each party and a Chairman appointed by the President. In addition to regulating interstate communications by wire and radio, the FCC charter states that the FCC’s purpose includes national defense and promoting the safety of life and property through wire and radio communications. The FCC has been assigned the Primary Mission Essential Function of maintaining ‘Operational Communications’ which is to ‘ensure continuous operations and reconstitution of critical communications systems and services.’

The FCC organized the Public Safety & Homeland Security Bureau in 2006 in the wake of Hurricane Katrina, pulling together pre-existing parts from other parts of the Commission to create a new, synergistic organization. The Bureau licenses and regulates public safety communications for over 30,000 licensees, police departments, state systems, sheriffs, fire departments and so on. We have a major policy responsibility for 9-1-1 systems, requiring the phone companies, including cable and Voice Over Internet Protocol (VoIP) telephone service, to provide 9-1-1 service. The Bureau analyzes the reliability of all legacy communications networks and requires the carriers to submit outage reports to us for major outages and that requirement was recently expanded to include VoIP telephone service. The Bureau maintains a world-class High Frequency Direction Finding Center with 14 HFDF sites from Alaska to Puerto Rico, which is used primarily for resolving interference with commercial aviation circuits over the Atlantic and Pacific and has other uses as well. We have responsibilities during emergencies and disasters. Cybersecurity policy is a major priority of this FCC Chairman, and my Bureau has primary responsibility.

Let me tell you what the FCC does not do with regard to cybersecurity: we do not do cyber defense; we don’t do cyber crime; we do not do cyber incident response. The FCC does have a unique relationship with the companies that operate the core of the Internet (telephone companies, wireless carriers and cable systems for instance) and that relationship can be a useful tool in cybersecurity. The FCC has always been interested in the reliability and the security of communications networks and that continues as we move rapidly into a broadband world.

Slide 4

The world has grown dependent on the rapidly growing broadband communications infrastructure.   Banking and commercial sectors, the energy sector, medical and educational establishments and all levels of government depend on the reliability and security of broadband communications networks to securely move vast amounts of data.   However, while our daily lives have become reliant on broadband communications, the networks and platforms on which broadband users rely contain vulnerabilities that make operator error and malicious cyber attack possible.

Tackling the challenges to Internet security is crucial, because the opportunities opened by the

Internet are immense. Our economy has become reliant on the Internet. Approximately $8 trillion are exchanged over these wired and wireless networks each year, and that is growing.

As Chairman Genachowski said in a cybersecurity speech at the Bipartisan Policy Center on February 22, “The online marketplace is the new Main Street in America.” Millions of people are involved in e-commerce, using websites like eBay and Amazon to buy or sell products.

The immense opportunities created by the Internet are real and are proportional to the formidable security challenges that are even now sapping our wealth, intellectual properties, privacy and identities.

I will guess that you are among the 150

million Americans who’ve shopped or banked online.   Organized crime syndicates are actively trying to dupe you, your family and friends into giving them your credit card information. 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 between $1.5 million to $36.5 million.

According to a Symantec survey, three-quarters of small and medium businesses report being affected by cyber attacks in the past 12 months.

The security vulnerabilities of the Internet and our digital infrastructure pose threats to our physical safety as well.   Our energy grid, water systems, and air traffic control rely on our digital infrastructure for their day-to-day operations.

The cyber threat is growing. Earlier in 2012, FBI Director Mueller warned that “Down the road, the cyber threat will be the number one threat to the country,” surpassing the dangers of terrorism.

The lack of security has real and hidden costs. We will pay the price in the form of diminished safety, financial vulnerability, lost privacy, lost jobs, and lost money -- hundreds of billions of dollars potentially lost to digital criminals.

Protecting user privacy is a crucial touchstone when working to ensure secure communications networks. We do not have to compromise privacy to improve online security. Privacy and security are both essential to consumer confidence, adoption of broadband and to fulfilling the promise of the Internet. We can and must improve online security while protecting individuals' privacy.

Again, Chairman Genachowski has stated clearly, "The openness of the Internet is a fundamental principal that must be preserved. It will not be compromised for security."

Slide 5

As the nation's expert agency on communications, the FCC has a long history of engagement on network reliability and security, working with commercial communications providers, wired and wireless, our partners in government agencies and other industry stakeholders to develop industry-based, voluntary best practices that improve security and reliability.

Slide 6

In 2011 we focused the work of our federal advisory committee the Communications Security, Reliability, and Interoperability Council (“the CSRIC”) on the new security challenges we face.   This Council and its predecessors have been working on cybersecurity issues for over ten years. In fact, in 2001, the Network Reliability and Interoperability Council, a predecessor of CSRIC, was one of the first federal entities to develop cybersecurity best practices.   CSRIC has made positive, substantive contributions to cyber and other security and reliability issues on a regular basis ever since.

The CSRIC now is made up of over 50

industry leaders from the private sector, academics, engineers, and federal partners. Its membership includes personnel from companies working every day to build and expand Internet infrastructure and services, from Verizon and Cox to Amazon and PayPal. It includes experts like Internet pioneers Steve Crocker and Michael O'Reirdan. CSRIC includes federal experts like Donna Dodson of NIST and Dr. Bryan Done of DHS, as well as representatives from state and local public safety entities.

Implementing a recommendation of the National Broadband Plan, in March, 2011, we tasked the CSRIC with making recommendations to help address critical Internet security vulnerabilities. We identified three areas where action is required to protect the Nation's communication's infrastructure: the Domain Name System, Border Gateway Protocol and the botnets, which cause distributed denial-of-service attack.   Since then, CSRIC's members have taken this responsibility seriously, working on their own and engaging intensely with other stakeholders.

Slide 7 and Slide 8

On the issue of DNS, the CSRIC is developing best practices that will guide ISPs' DNSSEC implementation.

Slide 9 and 10

To tackle BGP security, we have asked the CSRIC to develop a core set of voluntary best practices that would expedite the implementation of secure routing protocols and develop best practices to minimize the likelihood and impact of

BGP exploits. These best practices will be the products of the lessons learned from past problems and deliberate attacks. The CSRIC has also been asked to develop performance metrics to measure the effectiveness of its work.

Slide 11 and 12

Finally to address the threat of botnets, the CSRIC is proposing a voluntary Code of Conduct for ISPs. This Code of Conduct will identify best practices that can be applied by ISPs to provide a critical baseline of security to all Internet users.

Slide 13

The first set of CSRIC recommendations will be presented at the March 22nd meeting, which will be held at FCC headquarters and is open to the public.

Since more than 80% of the Internet is owned and operated by commercial companies, we recognize we must work with industry and that the first and best response to cyber threats may not be government intervention to dictate security standards for private companies. A better first response is to convene and facilitate efforts to identify and solve problems with engineers and other experts from industry, academia, NGO's as well as governmental partners.

This multi-stakeholder approach, which recognizes that the private sector is the front line, has worked throughout the Internet's history to address key challenges. And it continues to be the best approach for securing our networks while preserving the Internet as an open platform for innovation and communication.

Last month, in a speech at the Bipartisan

Policy Council, FCC Chairman Genachowski outlined the plans developed by the CSRIC and called on industry leaders to support these efforts. The Chairman’s speech was met with widespread support. The commitments we have received thus far from the private sector to work with us in combating these threats is a huge step forward, but is still only the beginning. We must remain vigilant to these ever changing threats as we seek to secure the communications networks that grow ever more dependent on broadband technology.

This effort with regard to ISPs is just one facet of a larger effort by the Department of Commerce, through NIST and the Department of Homeland Security. Under the President’s leadership, multiple agencies have launched initiatives to bolster our cyber defenses, including important efforts by the Department of Homeland Security, the Department of Commerce and NIST, and the Department of State.

DHS has created the National Cybersecurity and Communications Integration Center, which is a 24/7 watch and warning system, and is also leading the “Stop. Think. Connect.” campaign to better educate the public on how to make safe choices online.

The Commerce Department, NIST, and GSA are working together on the new National Strategy for Trusted Identities in Cyberspace, which aims to prevent online identity theft and make e-commerce more secure.

At the FCC, we have worked closely with our partners at other agencies. As the nation's expert agency on communications, the FCC has a long history of engagement on network reliability and security, working with commercial communications providers, wired and wireless, to develop industry-based, voluntary best practices that improve security and reliability.

Of course, the world is moving quickly toward IP-based communications, which introduces a host of new challenges. As we continue to do our work to promote secure communications networks, the rapidly changing landscape makes it that much more essential that we work in partnership with all stakeholders.

Slide 14

Most of what I have mentioned relates to network security, but another critical and closely related factor is network reliability. In the U.S., we have a widely recognized expectation that when we pick up a telephone, there will be a dial tone. And even though you may occasionally have a gap in cellular coverage, if you have coverage, you have an excellent expectation that your call will be connected. Not every other country has that expectation. One reason is, I hope, that U.S. providers have high standards for customer service. Another reason for the high standard is that the FCC does provide some accountability for the customers as well as best practices for the carriers. The FCC has been very active in working to improve network reliability in our network outage reporting system or the NORS program. The outage reporting principle is very similar to a principle I learned in our Armed Forces: do not expect what you don’t inspect.

Beginning in 2006 the FCC required carriers to report to us any time they suffered a large outage. The threshold is large: 900,000 user-minutes. So, if a carrier has 30,000 potential users who are unable to complete calls for 30 minutes, the threshold is breached and a report must be filed with the FCC.

We get a great deal of data from these reports and are able to look across the networks to see if there are trends or anomalies that lead to root causes. We sit down with the carriers and work on solutions. I will give you an example. A year ago in January, there was a huge snow storm right at the evening rush hour. Motorists were trapped on highways, and they all used their cell phones to call 9-1-1 at the same time. Thousands did not get connected. Everyone at first thought that the cause was simple that the circuits were jammed, but by analyzing the data from the carrier involved, we were able to detect the interaction of two devices in the system that could fail in similar situations in other networks. So, not only was that carrier's network problem corrected, so were other networks which had similar equipment.

The NORS outage reporting system has been shown to make improvements as much as 50% in reliability. In February, the Commission voted to extend our mandatory outage reporting rules to Voice Over Internet Protocol (VoIP), a major step forward, especially since approximately 31 percent of residential wireline subscribers have interconnected VoIP service. We expect that the extension of these outage reporting rules to VoIP will spur similar improvements in VoIP reliability.

Slide 15

I appreciate the opportunity you've given me to speak to you today; and I hope I've been about to give you just a bit of insight into the effort the FCC is making to secure the Nations' communications networks. We look forward to working with you in these ongoing efforts.