FCC CHAIRMAN JULIUS GENACHOWSKI
PREPARED REMARKS ON CYBERSECURITY
BIPARTISAN POLICY CENTER
WASHINGTON, DC
FEBRUARY 22, 2012

Today, I will address how cyber attacks pose a critical threat to our economic future and national security, and how the FCC and our federal partners are working with broadband providers and other stakeholders to develop smart, practical, voluntary solutions to tackle key threats to our cybersecurity. These steps are consistent with the long-standing multi-stakeholder approach that has enabled the Internet to flourish as an open platform for communication and innovation.

In particular, I'm calling on a broad range of Internet stakeholders to take concrete steps to address three significant cyber threats – botnets, domain name fraud, and IP hijacking.

With each of these issues, engineers and other experts from industry, academia, and non-profit organizations have worked with the FCC through our advisory council CSRIC to identify important measures that will materially improve our security and bolster the broader endeavors of our federal partners.

Tackling the challenges to Internet security is so important, because the opportunities of the Internet are so great.

Broadband Internet – over wired and wireless communications networks – has transformed our economy and society, opening up a new world of broad opportunity.

$8 trillion are exchanged over these wired and wireless networks each year, and growing. If you shut down the Internet, you'd shut down our economy.

The online marketplace is the new Main Street in America. More than 1 million entrepreneurs around the country are selling their products on platforms like eBay and Amazon.

And all of this online innovation and investment is creating jobs -- jobs not only at new tech companies, but at small and other businesses from coast-to-coast and in between.

The Apps Economy alone, which barely existed in early 2009, has now created nearly 500,000 new jobs.

Hundreds of thousands of additional jobs are expected to be created as broadband communications infrastructure gets built out to meet the growing data demand, particularly from mobile communications and cloud connectivity.

And broadband's benefits go beyond jobs and our economy.

The Internet is driving revolutionary breakthroughs in areas like health care, with remote monitoring and diagnostics; education, where broadband powers interactive digital textbooks and connects students anywhere to teachers and tutors who can help them learn; public safety, where next-generation 9-1-1 will allow first responders to receive texts, photos, and videos from emergency scenes, and – just last week – Congress funded not only progress toward Next Gen 9-1-1- but an important 9/11 Commission recommendation: a national mobile broadband network for public safety.

And of course the Internet is expanding and invigorating the public square, where digital tools are providing new ways of engaging with our government and with one another.

No question, the opportunities created by the Internet are real, and so are the security challenges.

Let's say you've got a home computer. There are bad actors out there right now trying to access your computer. If cyber criminals infect your computer with a virus, they could control it remotely, using it as a tool to send spam to all your personal contacts, and even to shut down web sites you rely on. If your computer gets hacked, all of the information on your computer – your family pictures, your private documents -- could be wiped out.

And that's not all.

Maybe you're one of the 150 million Americans who've shopped or banked online. There are organized crime syndicates trying to dupe you into giving them your credit card information. In fact, an estimated 8.4 million credit card numbers are obtained fraudulently online every year.

These costs can build on themselves. If consumers lose trust in the Internet, this will suppress broadband adoption and online commerce and communication, and all the benefits that come with it.

That's true for ordinary consumers and citizens, and it's true for small businesses.

The Internet provides new opportunities for small businesses to expand their markets and lower their costs, but cyber threats risk undermining the opportunities. According to a Symantec survey, three-quarters of small and medium businesses report being affected by cyber attacks. Last year, I met the owner of a local construction company, whose bank account was hacked through an email phishing scheme. His business lost tens of thousands of dollars.

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. Last month, 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.

If we fail to tackle these challenges, we will pay the price in the form of diminished safety, lost privacy, lost jobs, and financial vulnerability -- billions of dollars potentially lost to digital criminals.

It's important to pause and note the relationship between the Internet's success and these new threats. The potential harm of cyber attacks is so great because the Internet has become such a key platform for innovation, economic growth, and opportunity -- delivering more and more value to people everywhere, every day.

So as stakeholders address the challenge of cybersecurity, it's vital that we preserve the ingredients that have and will fuel the Internet's growth and success. Specifically, it's critical that we preserve Internet freedom and the open architecture of the Internet, which have been essential to the Internet's success as an engine of innovation and economic growth.

Preserving the openness of the Internet is not a concern to be balanced with security risks, it is a guiding principle to be honored as we seek to address security challenges.

Privacy is a similarly important principle. There are some who suggest that we should compromise privacy to enhance online security. This too is a false choice. Privacy and security are complementary – both are essential to consumer confidence and adoption of broadband. We can and must improve online security while protecting individuals' privacy.

A third key component for problem-solving in this area: the multi-stakeholder model. Like so many other Internet-related challenges, solutions to cyber threats will require the multiple stakeholders of the Internet community to work together and develop practical solutions to secure our networks. This approach has been fundamental to the Internet's development, and I believe it is the right course for the Internet's future.

The opportunities of the Internet, the problem of cyber attacks, and the need to solve these challenges consistent with long-standing Internet policy principles have all informed a number of important cybersecurity initiatives across the private sector as well as government.

Only weeks into his administration, President Obama initiated a 60-day review of America's cyber defenses – reaching out to members of industry and academia, as well as privacy and civil liberties experts.

The President established an Office of Cybersecurity within the White House and appointed Howard Schmidt as the nation's Cybersecurity Coordinator.

In May 2011, the White House submitted its legislative framework to Congress, and just last week bipartisan legislation was introduced in the Senate.

Also in May, the President released America's first International Strategy for Cyberspace, stating: "While offline challenges of crime and aggression have made their way to the digital world, we will confront them consistent with the principles we hold dear: free speech and association, privacy and the free flow of information."

The strategy emphasizes the importance of multi-stakeholder mechanisms and private-sector collaboration to advance cybersecurity.

One month later, the U.S. was one of 34 countries that endorsed the Organization for Economic Cooperation and Development's principles for Internet policymaking, which emphasize the importance of multi-stakeholder cooperation to promote network 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 its National Institute of Standards and Technology (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 the General Services Administration (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.

Last year, working with the Small Business Administration, the Chamber of Commerce, the National Urban League, and many private technology companies, we developed and released a Cybersecurity Tip Sheet for small businesses, describing a number of commonsense steps small businesses can take to increase their security. Password protecting your Wi-Fi router is one example.

Working with our partners, the FCC also released an easy-to-use tool – our Small Biz Cyber Planner – to help small businesses develop a customized cyber plan.

Our next step is to expand the distribution of this tool and the tips, working with partners inside and outside government.

In 2011 we also accelerated the work of our CSRIC, the FCC's Communications Security, Reliability and Interoperability Council. This Council and its predecessors have been working on cyber security issues for some time. In fact, in 2001, the Council -- then called the Network Reliability and Interoperability Council -- was one of the first federal entities to develop cybersecurity best practices. And 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 industry leaders, academics, engineers, and federal partners. Its membership includes companies working every day to build and expand Internet infrastructure and services, from Verizon and Comcast to Amazon and PayPal. It includes experts like Internet pioneers Steve Crocker and Michael O'Reirdan. And it includes federal experts like Donna Dodson of NIST, and Dr. Pete Fonash 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, I tasked CSRIC with making recommendations in the spring of 2012 to help address critical private-sector Internet security vulnerabilities.

Since then, CSRIC's members – starting with its working group leaders – have taken this responsibility seriously, working on their own and engaging intensely with our agency experts. Based on that work, I want to describe three critical cybersecurity threats -- botnets, Internet route hijacking, and domain name fraud -- and suggest steps to help significantly reduce those threats.

These solutions were developed through a multi-stakeholder process that recognizes that the best response to these threats is not government dictating security standards for private companies. This is the type of approach the FCC is taking in this area -- convening and facilitating efforts to identify and solve problems with engineers and other experts from industry, academia, and non-profit organizations, not regulatory action. This multi-stakeholder approach, which recognizes that almost all of our broadband infrastructure is owned and operated by the private sector, 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.

Let's start with botnets.

Botnet is shorthand for "robot network." They are created by cyber criminals who distribute a virus, better known nowadays as malware, over the Internet.

A user's PC or a company's server can become infected by someone unsuspectingly opening an email or downloading a file, installing a piece of malicious software on your

computer. This software allows bad actors to control your computer remotely.

These infected computers are commonly known as bots or Zombie PCs, and most people don't realize when their computer has become a bot.

How many zombie computers are out there? It's hard to say, but one botnet controlled approximately 12 million computers in as many as 190 countries.

Criminals commonly use these botnets to launch cyber attacks. They can direct the zombie computers to send millions of simultaneous requests to a target website, crashing the site.

Botnets have been central to a very large percentage of the website crashes you've heard of, and that you haven't.

For the average consumer, the consequences can be equally devastating. Bots are used to relay massive amounts of spam. Bots can be used to steal passwords and financial information, putting an individual's identity at risk.

So what can we do about botnets?

Consumer education is a key piece of the solution. New technologies require new norms and practices. Empowering consumers with information and tools can help them secure their computers in this rapidly changing environment.

Internet Service Providers cannot do this alone, but ISPs can play a significant role in the battle against botnets. They can increase customer awareness so that users can look for signs that their computers are being used as bots, detect infections in customers' computers, notifying customers when their computers have become infected, and offer remediation support.

Of course, ISPs can and must do this in a way that does not compromise consumers' privacy.

Comcast and CenturyLink have already taken the lead in developing and promoting solutions like this. If other ISPs employed similar best practices, it could significantly reduce the botnet threat.

Today, I'm calling on all ISPs, working with other stakeholders, to develop and adopt an industry-wide Code of Conduct to combat the botnet threat and protect the public. This Code of Conduct would be a major step forward and a significant complement to the Administration's broader efforts against botnets.

Botnets are the first significant problem we've targeted. The second is Internet route hijacking.

The Internet is a network of networks. Connectivity between these networks is based on an implicit trust that is the Internet's biggest strength, but can also be a major weakness.

The protocol that enables seamless connectivity – known as Border Gateway Protocol or BGP -- doesn't 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, perhaps untrustworthy, 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 data before it arrives at its intended destination.

We saw this risk in 2010, when traffic to 15% of the world's Internet destinations was diverted through Chinese servers for approximately 18 minutes.

It is impossible to calculate the true costs of an incident of this magnitude.

Misrouted traffic, whether intentional or accidental, is clearly unacceptable.

How do we fix it?

Network operators need to adopt secure routing standards, and engineers – including leading engineers involved in the development of the Internet – are making real progress on developing these technical standards in a way that will protect individual privacy and secure Internet routing.

I strongly urge ISPs to support the development of secure routing standards and plan to implement them when they are ready. Costs of implementation can be minimized by putting in place the new technical standards during routine hardware and software upgrades. The benefits of ISPs taking these steps to eliminate accidentally misrouted traffic would be enormous.

The third major problem is domain name fraud.

As more and more of us are aware, the Internet is built using the Domain Name System – or DNS. DNS is essentially a digital phone book for the web. Servers are filled with identifying information for web sites, which is used to direct people where they want to go.

The challenge is that the DNS has vulnerabilities that can allow the identifying information to be changed. And when bad actors change the identifying information, computer users attempting to go to one website can get misdirected to a fraudulent website.

Often the fraudulent websites are designed to look exactly like the legitimate website that the user intended to visit. Users have no idea that they are not working with legitimate

websites, and unwittingly provide the operators of the fraudulent websites with financial and personal information. You could kind of think of it as the Little Red Riding Hood problem.

In 2009, a bad actor managed to pull a bait-and-switch with the website for one of Brazil's biggest banks. The bank's customers found themselves on a fake site that looked exactly like the real one. Customers' user names and passwords were stolen for four hours until the crime was discovered.

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

The good news is that the Internet Engineering Task Force has already developed a series of security extensions to the DNS, which are designed to address these vulnerabilities. The IETF is a highly respected, independent, open standards organization comprised of engineers and other experts that has worked on Internet standards since the 1980s. Their solution is called DNSSEC, and it's been endorsed by Internet pioneers, including Rodney Joffe, Vint Cerf, and Steve Crocker, as well as Internet organizations like the Internet Society.

DNSSEC was designed with privacy in mind and it can and must be implemented in a way that protects individual privacy.

The standards for DNSSEC are well established and are already being deployed by government entities. But adoption in the private sector has been slow.

If they adopt DNSSEC, ISPs can provide a real and tangible benefit to the consumers and businesses that rely on them. DNSSEC is ready to be implemented. Indeed, at least one major U.S. ISP has already completed implementation of DNSSEC.

I urge all broadband providers to begin implementing DNSSEC as soon as possible.

Domain name fraud, IP hijacking, and botnets pose a significant threat to our economy and our digital society. They aren't the only cyber threats we face, but experts agree they represent a very significant part of the problem. FCC staff estimates that the costs of these cybercrimes is at least tens of billions dollars annually, and growing.

The stakes are high, but solutions to these threats are in sight. I hope and expect stakeholders will rise to the challenge.

I thank the leaders of CSRIC and all of its members for participating in this important process, which complements the measures being considered by Congress. And I thank our federal partners for participating in CSRIC, even as they drive many other important initiatives to tackle cyber threats.

With all of the key stakeholders working together, I am confident we can make a real

difference in increasing the security of the Internet and harnessing its enormous opportunities.

Thank you.