FCC CHAIRMAN JULIUS GENACHOWSKI
PREPARED REMARKS ON CYBERSECURITY
MEETING OF THE COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL (CSRIC)
WASHINGTON, DC
MARCH 22, 2012

Before discussing today's reports, I want to acknowledge all of the outstanding work CSRIC does to enhance the security and reliability of our communications networks.

CSRIC of course is the FCC's Communications Security, Reliability and Interoperability Council. I was pleased to charter this current iteration of CSRIC back in March 2011, and the talent and expertise on the current Council is world-class – with industry leaders representing a broad cross-section of the broadband economy; world-class engineers both who helped invent and develop the Internet and who understand the latest technologies and trends; award-winning academics and thought leaders; and dedicated federal partners from across government.

CSRIC works on a variety of topics, ranging from next generation 9-1-1 to, of course, cybersecurity.

In fact, CSRIC has worked on developing solutions to our cybersecurity challenges going all the way back to 2001, when an earlier panel developed one our government's first set of cybersecurity best practices.

When we re-chartered CSRIC last year, I tasked this panel with developing practical, concrete steps to reduce the threat of cyberattacks.

Last month, at the Bipartisan Policy Center, based on the work of CSRIC, I called for industry action on three specific cybersecurity challenges: botnets, Internet route hijacking, and domain name fraud.

Today, CSRIC and many industry players are answering this call to action.

Thank you, Glen for these important CSRIC reports.

Thanks to all the CSRIC members who participated in the working groups, in particular, the Chairs of the specific panels – Steve Crocker, Michael O'Reirdan, and co-chairs Andy Ogielski and Dr. Jen Rexford.

As this group knows all too well, cyber attacks pose a critical threat to our economic future and national security.

To put the scale of this challenge in some perspective, experts reported recently that the majority of all Internet traffic is non-human – it's bots, automated spam, and hacking software.

There are basically three prime targets for cyber criminals.

The first is government-owned networks.

The second is the networks that sustain vertical industries like financial services and our energy grid.

The third area is commercial networks, wired and wireless, which are what most Americans are using every day to send e-mails, pay bills, or shop online.

Our work together has been focused on the third category.

As the nation's expert agency on communications networks and technology, the FCC has always had as a fundamental part of our mission the security and reliability of communications networks.

At the FCC we have taken steps to enhance the ability of small businesses to defend themselves against cyber attack. For example, we've worked with external partners to create an easy-to-use tool – our Small Biz Cyber Planner – to help small businesses develop a customized cyber plan. This effort has included the Chamber of Commerce, the National Urban League, Symantec, McAfee, Thomson-Reuters, and the Small Business Administration, and we are grateful for their work, which helped lay some groundwork for today's action.

The work of CSRIC is the FCC's most significant effort yet to enhance cybersecurity.

We called on you to develop cybersecurity solutions, real steps that will materially enhance our security, and to do it in a way that preserves the ingredients that have and will fuel the Internet's growth and success.

That means solutions that 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. As I've said before, preserving the openness of the Internet isn't 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 vital principle. And while 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 in the Internet and to 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. Solutions to cyber threats require the multiple stakeholders of the Internet community to work together and develop practical solutions to secure our networks. The goal isn't regulation; the goal is solutions – and the history of the Internet tells us that the multi-stakeholder model can produce solutions. It continues to be the best approach for securing our networks while preserving the Internet as an open platform for innovation and communication.

The reports you adopted today identify smart, practical, voluntary solutions that are consistent with these principles, will materially improve our cybersecurity, and bolster the broader endeavors of our federal partners.

On botnets, CSRIC has now developed a voluntary U.S. Anti-Bot Code of Conduct – the ABC – to reduce the threat of bots in residential broadband networks. The Code includes steps to better detect bots in customer computers, and to notify consumers when their computers have been infected. It includes steps to educate consumers so that users can look for signs that their computers are being used as bots. And it recommends making tools available to help remediate bots. For example, customers of CenturyLink and Comcast can already go to those companies' websites and download a tool that will scrub your computer if it's infected by malware.

On domain name fraud, CSRIC endorses new steps toward implementing expert-designed security improvements to the Domain Name System – DNSSEC. In particular, CSRIC recommends that ISPs use DNSSEC to give their customers the ability to validate the services they use on the Internet. For example, ISPs that implement CSRIC's recommendations will be providing customers with the means to verify the authenticity of websites they visit.

On Internet route hijacking, the report calls on network operators to develop and adopt new technical standards that will secure Internet routing.

The secure Border Gateway Protocol standards would establish a certified registry that will enable ISPs to validate the authenticity of routing information, securing the foundations of trust between networks, which has been so essential to the Internet's success.

I want to thank CSRIC's members who helped develop these solutions. You've laid out a blueprint for addressing some of the biggest threats to our digital economy.

Now, as all of you know, this town is littered with expert reports filled with smart recommendations that wind up at the bottom of a pile. That's not at all what CSRIC has adopted today. Not only has CSRIC laid out a plan for action; many of your member companies are making a commitment to act.

I want to recognize the companies that have already committed to implement the core recommendations of all three reports. Please stand as I call your company's name. AT&T, CenturyLink, Comcast, Cox, Sprint, Time Warner, and Verizon.

I'd also like to acknowledge T-Mobile, which supports all three recommendations and will be implementing DNS-SEC, which is the one that applies to them.

So we're not just issuing three reports today. We're talking about companies that serve more than 80% of the country's Internet users committing to meaningful solutions to significant cybersecurity challenges.

We expect that other companies will commit to implementing these recommendations as well, and that CSRIC's voluntary cybersecurity measures will soon become the industry standard operating procedures.

These actions will have a significant positive impact on Internet security.

If you own a PC, you'll be significantly better protected against your computer taken over by a bad actor, who could destroy your private files or steal your personal information.

If you shop or bank online, you'll be significantly better protected against being directed to an illegitimate website and having your credit card number stolen.

If you manage a business, you'll be significantly better protected against your Internet traffic being misrouted, which could allow cyber criminals to steal valuable intellectual property.

Implementing these recommendations will reduce the risks of cyber crimes that cost U.S. businesses and consumers billions of dollars every year and will enhance the security of this platform that is increasingly integrated into every aspect of our economy and society.

Today's reports and commitments are a significant step forward, but there is still much more work to be done.

The actions I've talked about will help tackle serious threats that exist now. The problems of botnets, domain name fraud, and IP route hijacking will not go away if unaddressed.

And meanwhile, technology continues to change, consumer behavior continues to evolve, and new cyber threats will develop.

The bad guys won't stop innovating, and that means the good guys can't stop innovating either. Indeed, we need to accelerate innovation, and we need to do so across all parts of the broadband ecosystem that have a stake in cybersecurity – including ISPs, search engines, designers of operating systems, security software developers.

We need new ways to incentivize innovation in cybersecurity. We also need to ensure that there are appropriate levels of R&D going into cybersecurity.

In addition to greater engagement from every segment of the broadband ecosystem on cybersecurity, there are additional steps CSRIC can take, and I'm looking forward to working with CSRIC on these.

Within today's recommendations, there can be multiple ways to take action.That's great, but we need to understand which solutions work best. And so I've tasked CSRIC with developing metrics to measure the effectiveness of cybersecurity solutions.

I'm also asking CSRIC to ensure that all solutions they develop are consistent with consumer privacy.

CSRIC's work is significant. You've proven that you can come up with concrete solutions to concrete problems, and established a process and a set of principles for identifying problems and tackling them.

This fits very well into the set of important cybersecurity initiatives across government.

To talk about the administration's comprehensive efforts, we are fortunate to be joined by the Senior Director for Cybersecurity Policies on the National Security Council staff. Please join me in welcoming Miriam Perlberg.