PREPARED REMARKS OF FCC CHAIRMAN GENACHOWSKI
CENTCOM CONFERENCE: "ADVANCING CYBER SECURITY THROUGH REGIONAL COOPERATION"
HERNDON, VA
NOVEMBER 14, 2012

Now let me talk for a few minutes about the FCC's efforts on cybersecurity.

Tackling the challenges to network and Internet security is extremely important. It's so important because the benefits and opportunities of the Internet are so great.

Broadband Internet – over wired and wireless networks – has transformed our economy and society, opening up a new world of uncharted opportunity. Eight trillion are exchanged over these wired and wireless networks each year, and growing. The Internet is driving productivity gains, economic growth, and job creation. If you shut down the Internet, you'd shut down our economy. That's increasingly true around the world.

The Internet presents vast new opportunities, but also new dangers. The challenge is to tackle the dangers without undermining the opportunities. It's not an easy challenge.

One of the first steps, I think, is to break down the challenge into categories that allow for meaningful discussion and problem solving.

One division of the threats is into three categories of networks. The first is government-owned networks. The second is the networks that sustain vertical industries like financial services and our energy grid. And the third area is commercial networks, wired and wireless, which are what most people are using every day to send e-mails, pay bills, or shop online. Commercial networks are also increasingly integrated with the second category – vertical networks of critical infrastructure.

At the FCC we've been engaged in all three areas. For example, we've been advising both the White House and Congress on various cybersecurity matters, including legislation that's been in front of Congress.

Primarily, we've been focused on the third category – commercial networks. 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 commercial communications networks.

So what is the FCC doing proactively to make our commercial broadband networks more secure?

Let me start with one example of how doing relatively easy things - what we call "low hanging fruit" - can have a big impact. I'm talking about helping small businesses improve their security.

Don't let the name fool you. Small businesses are a huge part of the U.S. economy. They employ more than half of all private sector workers.

Increasingly, small businesses depend on broadband Internet to reach customers and boost productivity.

But in the U.S., 83% of small businesses don't have cybersecurity protection plans. And too many U.S. small businesses are not doing obvious things to guard against cyber attacks, such as encrypting their Wi-Fi networks or better password protection.

So the FCC helped build a coalition that included government partners like the Small Business Administration, non-government organizations like the U.S. Chamber of Commerce and the National Urban League, and several major private technology companies to try to tackle this problem. Working together, this group has develop easy-to-use tools and resources to help small businesses protect themselves from cyber attacks, including basic materials with easy-to-understand steps small businesses could take to improve their security and derive the many benefits of being online.

Now I'd like to talk in a little more detail about a significant multistakeholder initiative the FCC drove last year. This involved Internet Service Providers and many others. The goal was to identify and tackle concrete, high priority security challenges.

Last year, I tasked a coalition of FCC partners and stakeholders with making recommendations to help address three concrete challenges that our work, and the work of others, had identified: botnets, Internet route hijacking, and domain name fraud.

This was a deliberate choice. I didn't give the general charge of tackling cybersecurity. I gave this group three concrete areas in which we wanted progress and solutions. I encourage this approach to others. I fear that a boil-the-ocean approach is less likely to lead to material real-world progress.

The group that developed these solutions is the FCC's Communications Security, Reliability, and Interoperability Council – or CSRIC. CSRIC is an advisory council to the FCC that is made up of industry leaders, academics, engineers, and federal partners. 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.

CSRIC's current membership includes companies working every day to build and expand Internet infrastructure and services, from Verizon and Comcast to Amazon and PayPal. It includes outside experts from academia. And it includes federal experts from multiple agencies, as well as representatives from state and local public safety entities.

Early in 2012, CSRIC issued a series of smart, practical recommendations on the three issues I mentioned.

On botnets, CSRIC developed a voluntary U.S. Anti-Bot Code of Conduct 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 *remediate* bots, including educating consumers so that users can look for signs that their computers are being used as bots.

On domain name fraud, CSRIC endorsed new steps toward implementing expert-designed security improvements to the Domain Name System – DNSSEC. In particular, CSRIC recommended 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 CSRIC report called on network operators to develop and adopt new technical standards that will secure Internet routing. The standards would establish an authoritative 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.

CSRIC laid out a concrete plan for action in three key areas, and we were able to accomplish more than that. In conjunction with issuance of the CSRIC report, ISPs that serve roughly 90% of the country's Internet users committed to implementing the recommendations.

In all of our work to enhance online security, we have made sure these efforts are consistent with key values that have fueled the Internet's growth and success.

One of those values is Internet freedom. Both President Obama and Secretary of State Clinton have spoken about how the open architecture of the Internet and the free flow of information online have been essential to the Internet's success as an engine of innovation, economic growth, and democracy.

Privacy is a similarly vital principle. The notion that we face a fundamental divide between privacy and security 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.

In the U.S., we've found that a key part of the recipe for driving investment and innovation that unleash new opportunities and greater prosperity is moving strongly to address security concerns, while always remaining true to these guiding principles.

Of course, technology continues to change, consumer behaviors continue to evolve, and new cyber threats will develop. Looking ahead, an increasingly important area that we're focusing on is securing advanced mobile devices, including smartphones.

Worldwide, more people are getting online with mobile devices than with PCs. Consumers are increasingly installing different types of apps on their smart devices and browsing mobile websites, while most are unaware of the potential risks created by their behavior and the best practices to mitigate them. Consequently, we're concerned that consumers are generally not taking adequate precautions against the threats that can harm their devices and exploit the information on their devices.

These mobile devices we use to help run our lives and businesses are really just mobile computers. We need to be thinking about how to make sure the risks to our PCs—like botnets—don't make their way onto our smartphones and tablets. The FCC will be announcing concrete steps to tackle this issue in the coming weeks.

In each of these areas, we are working through a similar, highly effective model that I believe can be applied broadly: recruiting top talent to the FCC to focus on these issues, coordinating with multiple stakeholders, charging them with solving concrete problems, and honoring core Internet values we want to preserve.

When we talk about coordinating with multiple stakeholders, we're talking about two buckets.

First, it is essential that government collaborate with the private sector to solve these challenges.

Second, inter-agency collaboration is essential.

We're applying this collaborative approach in other critical public safety situations, aside from cybersecurity.

For example, the FCC recently supported America's Federal Emergency Management Agency (FEMA) and other government agencies in response to Hurricane Sandy, which devastated parts of New York and the New Jersey coastline, reporting daily on the state of the communications networks in the affected areas.

And it's the same collaborative model we used after the devastating earthquake in Haiti in 2010, where we worked in close coordination with FEMA, the branches of the U.S. military, and private companies to quickly restore communications to communities that had been cut off.

I had a good conversation with Brigadier General Baker last week about the importance of taking a similar approach in other areas - for example, cable landing stations, which are often controlled by private licensees, are also vital pieces of security infrastructure, and are often underprotected. We must work together collaboratively to tackle challenges like this.

I mentioned that in developing strategies to tackle cyber threats we have sought to protect the key values that have fueled the Internet's growth and success.

I'd like to close by discussing next month's World Conference of International Telecommunications in Dubai, which poses real challenges to these values.

As you know, that Conference will be reviewing the International Telecommunication Regulations, and cybersecurity issues have become a focus of discussion.

Since the 1990s, opening up global telecommunications markets to greater competition and private investment, and embracing a multi-stakeholder model of Internet governance has helped fuel massive deployment of communications infrastructure, contributing significantly to economic growth, job creation, and new opportunities in areas like health and education around the world.

The bipartisan position of the U.S. government is that the multi-stakeholder, market-based and consumer-driven model for international telecommunications and the Internet is working and will continue to be the best engine for growth and opportunity in these sectors, all over the world.

The U.S. supports, and will work for, continued growth and expansion of a vibrant, competitive international communications and Internet sector.

This will contribute to more innovation, entrepreneurship and economic growth, creating opportunity all over the world.

This is why we remain concerned about ongoing discussions about cybersecurity in the context of WCIT. Cyber threats are a growing issues, but one that is being addressed in a variety of multistakeholder fora.

Calls to add cybersecurity provisions in the International Telecommunication Regulations are misplaced and ultimately counterproductive. International regulations are simply too broad, too inflexible, and too slow to change to effectively address cybersecurity issues. And any attempt to draft a "one-size-fits-all" text could easily do more harm than good.

We believe it is important to have a successful WCIT, and we want to encourage other administrations to seek consensus and avoid extreme positions. We believe the Conference should take a pragmatic, flexible, and real-world approach.

On a final note, we at the FCC believe that the whole world benefits when countries work together to promote core ideas like competition, the free flow of data, and secure networks – pillars of the digital economy that drive economic growth, new opportunities, and global prosperity.

We also recognize that we have common challenges when it comes to seizing the opportunities of the digital age: challenges around broadband adoption and deployment, and maximizing the benefits of broadband in areas like health care, education, and public safety.

This is not a zero-sum game. We can learn from one another and all can benefit.

That's why we are committed to greater transparency at our agency, and making information about our policies and practices available online. And why we have also dedicated significant time and resources to direct engagement with our foreign counterparts, and the ongoing exchange of information.

I'm proud to say that we are actively engaged with your region as we have hosted 28 delegations from Bahrain, Egypt, Iraq, Jordan, Oman, Qatar, Saudi Arabia, United Arab Emirates, and Yemen during the last two years. We have a very active International Visitor's Program and we look forward to continuing our full engagement with the region.

Working together, I am confident we can make a real difference in increasing the security of the Internet and harnessing its enormous opportunities. I look forward to continuing what has been a tremendously valuable conversation.