Remarks of FCC Chairman Tom Wheeler
American Enterprise Institute
Washington, D.C.
June 12, 2014

Thank you to the American Enterprise Institute for convening this important discussion.

I'm honored to be part of a lineup with General Hayden, General Alexander, Chairman Rogers, Christopher Painter, FTC Commissioner Ohlhausen, and others.

I won't pretend to be an expert on national security, especially relative to the other speakers you will hear from today. But I suspect the reason you invited me today is because I do pretend to know a little something about networks, and our cybersecurity challenge is network-based. Since the FCC is the nation's network agency, I thought it might be appropriate to reflect on what I envision as the FCC's role in addressing network security for the communications sector in the Internet age.

In particular, I want to address how stakeholders in the communications sector – the sector on which all aspects of the digital economy depend – must create a new paradigm for cyber readiness. This begins with private sector leadership that recognizes how easily cyber threats cross corporate and national boundaries. Because of this reality, the network ecosystem must step up to assume new responsibility and market accountability for managing cyber risks.

The challenge is that this private sector-led effort must be more dynamic than traditional regulation and more measurably effective than blindly trusting the market or voluntary best practices to defend our country. The new paradigm for the communications sector must be real and meaningful. It has to work. The Commission's commitment to market accountability will help ensure that it does work. And, while I am confident that it will work, we must be ready with alternatives if it doesn't.

Now, let me pause right here. Before headline writers rush to interpret this as "FCC wants to regulate cyber," we need to put these statements in the context of a broader philosophy we've been practicing at the FCC. We believe there is a new regulatory paradigm where the Commission relies on industry and the market first while preserving other options if that approach is unsuccessful. The purpose of these remarks is to explain that concept as it applies to cybersecurity. Basically it boils down to this: identify public goals, work with the affected stakeholders in the communications industry to achieve those goals, and let that experience inform whether there is any need for next steps.

Our new information networks *are* the new economy. Earlier networks enabled ancillary economic activities. But our growth industries today are based on the exchange and use of digital information. As such, information networks aren't ancillary; they are integral. And their security is vital.

For all the ways the Internet has already transformed our lives, today's network revolution is constantly creating enormous new opportunities to grow our economy, to enhance U.S. competitiveness, and to improve the lives of the American people.

Yet, these changes also raise new security challenges – challenges that must be addressed if we hope to seize the opportunities.

Consider the Internet of Things. Every second, about 100 new "things" are connecting to the Internet – most of which are not people. Soon, we'll have refrigerators talking to milk cartons and sending a text message to pick up a new quart on the way home. Cisco forecasts that by 2020 – that's less than half a dozen years away – over 50 billion inanimate devices will be interconnected. Expressed another way, that's 50 billion new attack vectors.

Similar threats continue to grow with mobile apps, social networks, and the other realities of our rapidly evolving networked world.

And it's not as if cybersecurity weren't already complicated enough. Our cyber adversaries do not fit a particular profile. They run the gamut from those working on behalf of governments to steal trade secrets and intellectual property, to ideological non-governmental groups with malicious intent to harm critical infrastructure, to criminal organizations intent on wreaking havoc and making a profit, to individual hackers trying to steal private information.

The unfortunate reality is that our cyber adversaries worldwide are right at our virtual doors, ready to break in the moment they sense the opportunity to steal our valuable information – including personal information - and damage the networks on which we rely.

Everybody in this room understands that tackling the challenges of cybersecurity will require a joint effort. That means collaboration within the federal government; collaboration between federal, state and local governments, collaboration between the U.S. and foreign governments; collaboration between government and the private sector; and even inter- and intra-industry collaboration.

So what, exactly, is the FCC's role in this shared endeavor?

The FCC's responsibility to promote public safety and network security is fundamental. Our mandate is codified in the Communications Act, which tells us that the FCC was established for the purpose of, among other things, promoting the national defense, and the safety of life and property.

Allow me to get wonky for a moment. Our telecom law was last updated in 1996, early in the life of the new Internet Protocol world. I was there, and I can assure you no one foresaw then the scope of IP-based communications that we take for granted today.

But the beautiful thing about our communications law is the ability that Congress has given to this agency to face new circumstances. The drafters of the statute wisely spoke in terms of

effects such as the "public interest, convenience and necessity." While there are many proscriptive parts of the statute, it maintains at its core an effects-based orientation.

The challenge of the FCC is to deliver on the national security and public safety effects mandate as the networks that enable those effects evolve from analog to digital.

The FCC cannot abdicate its responsibilities simply because the threats to national security and life and safety have begun to arrive via new technologies. If a call for help doesn't go through, if an emergency alert is hijacked, if our core network infrastructure goes down, are we really going to say, "Well, that threat came through packet-switched IP-based networks, not circuit-switched telephony, so it's not our job…"?

We have unique, indispensable expertise and responsibilities when it comes to the communications sector. So long as I am Chairman, we will work diligently and strategically with all stakeholders to leverage that expertise and fulfill these responsibilities. Let me describe how I hope we will be able to build a new paradigm of proactive, accountable cyber risk management for the communications sector.

The New Consensus. First, the FCC must build upon past Federal and private sector work in cybersecurity.

Following President Obama's Cyberspace Policy Review in early 2009, a robust national dialogue helped create a new consensus for cybersecurity. Our nation chose proactive private sector cyber risk management – and all the corporate responsibilities and accountability that go along with that – over a traditional regulatory approach of prescriptive government mandates.

In February 2013, with the encouragement of many of the legislators who had fought in the trenches of those debates on Capitol Hill, President Obama issued an Executive Order, which brought structure to a private sector-driven cybersecurity standards process facilitated by NIST.

NIST's Framework for Improving Critical Infrastructure Cybersecurity prompted a depth of private sector engagement and trust that had not previously existed. The issuance of the Framework earlier this year has created a tremendous opportunity to make major, meaningful strides in cybersecurity.

The Framework is a flexible, adaptable approach to risk management that can be applied by companies of all types and sizes across all sectors. It is not a static checklist. The Framework's success will rely on proactive risk management, not reactive compliance with a cybersecurity to-do list.

We have our work cut out for us, but there is now a deep and broad consensus that this approach is the only workable strategy for securing commercial networks.

Growing cyber threats will test this proposition, so we must together seize the opportunity that the new consensus presents.

The FCC's New Paradigm. So how do we, as a regulator, ensure that the communications sector steps up to the challenge?

I come from the technology entrepreneur and investment world, and I take a business-and-technology oriented perspective to this policy question.

I firmly believe that we are not as smart, or as fast, or as innovative as the Internet. The pace of innovation on the Internet is much, much faster than the pace of a notice-and-comment rulemaking.

We live in an age when a few smart 20-year-olds in somebody's garage can render standard technology obsolete within months. And the same is true for the pace of threat technology.

We cannot hope to keep up if we adopt a prescriptive regulatory approach. We must harness the dynamism and innovation of competitive markets to fulfill our policy and develop solutions. We are therefore challenging private sector stakeholders to create a "new regulatory paradigm" of business-driven cybersecurity risk management.

This new paradigm must be based on private sector innovation, and the alignment of private interests in profit and return on investment with public interests like public safety and national security.

It needs to be more dynamic than rules, and – this is a key point – it needs to be more demonstrably effective than blindly trusting the market. "Demonstrably effective" will require a level of transparency that may make take some time to get used to, but the bottom line is that this new paradigm can't be happy talk about good ideas – it has to work in the real world. We need market accountability on cybersecurity that doesn't exist today, so that appropriately predictive and proactive investment is made to improve cyber readiness.

This is a big task, but it is an essential responsibility.

We will be guided by a top notch team, led by the Chief of our Public Safety and Homeland Security Bureau Admiral Dave Simpson.

We also have created new position of Chief Counsel for Cybersecurity to help Admiral Simpson navigate the legal and strategic considerations, and Senate Intelligence Committee veteran Clete Johnson is filling this role.

Rounding out the Admiral's leadership team is Jeff Goldthorp, who has worked on these issues at the Commission for more than a decade.

Agency-wide, our Bureau Chiefs and Office Heads are working with the Admiral to "bake" cyber into the DNA of the Commission. Our activities going forward need to consider vulnerabilities and impacts from cyber early on and throughout our FCC processes.

OK, so we have a new consensus, a new regulatory paradigm, and a new team. What does this mean in real terms?

Our work on cybersecurity in the communications sector will be guided by a set of principles.

- First and foremost is a commitment to preserving the qualities that have made the Internet an unprecedented platform for innovation and free expression. That means we cannot sacrifice the freedom and openness of the Internet in the name of enhanced security.

- Second is our commitment to privacy, which is essential to consumer confidence in the Internet. We believe that when done right, cybersecurity enables digital privacy – personal control of one's own data and networks.

- Third is a commitment to cross-sector coordination**.** We cannot address these threats in one-sector or one-agency silos. Particularly among regulatory agencies, we must coordinate our activities and our engagement with our sector stakeholders.

- Fourth, we continue support the multi-stakeholder approach to global Internet governance that has successfully guided its evolution, and we will oppose any efforts by international groups to impose Internet regulations that could restrict the free flow of information in the name of security. The digital economy is global, and this multi-stakeholder improvement in cyber readiness and market accountability will be a useful template for others and have positive impacts worldwide.

Guided by these principles, I have directed the FCC staff to organize our cyber activities around some central pillars:

First, Information Sharing and Situational Awareness. We are examining the legal and practical barriers to effective sharing of information about cyber threats and vulnerabilities in the communications sector. In order to protect companies and consumers against malicious cyber attacks and intrusions, companies large and small within the communications sector must implement privacy-protective mechanisms to report cyber threats to each other, and, where necessary, to government authorities. And for cyber attacks that cause degradations of service or outages, the FCC and communications providers must develop efficient methods to communicate and address these risks. We've witnessed great innovation and progress on these issues in the financial sector, where institutions of all sizes have worked together to develop ground-breaking practices for sharing cyber threat information to combat threats in real time. Such approaches can be a model for the communications sector to span the large risk and awareness gap between large and small, urban and rural providers. We are actively engaged with private sector Information Sharing and Analysis Organizations, and with our Federal partners – particularly DHS and the FBI – to increase the efficiency of threat information sharing and improve situational awareness. To be clear, we seek only to assist and support – not to replace or duplicate – existing private or public information sharing activities.

Second, Cybersecurity Risk Management and Best Practices. In 2011, our primary Federal advisory committee on these issues, the Communications Security, Reliability and

Interoperability Council (CSRIC) completed voluntary industry best practices pertaining to domain name security, Internet route hijacking, and an Anti-Bot Code of Conduct. This was important foundational work. These standards, if implemented broadly, would "harden" our nation's communications backbone against cyber threats with potentially wide-scale industry implications. In the coming weeks we will be seeking information to measure the implementation and impact of these industry-defined best practices. In business school, I learned, "If you can measure it, you can manage it." I look forward to learning more through these inquiries as to whether the private sector is taking this issue as seriously as it must.

Building on these efforts, CSRIC is presently hard at work developing risk management processes to tailor the NIST Cyber Security Framework for the communications sector. This particular effort, which features the active participation of over 100 experts from throughout the communications sector, is a landmark initiative – the central proving ground for whether our attempt to create a new paradigm will succeed. We are asking communications providers to work with us in setting the course for years to come regarding how companies in this sector communicate and manage risk internally, with their customers and business partners, and with the government. This will require a degree of transparency and assurance to give consumers, fellow providers, the market, and the FCC confidence that internal efforts are proactively addressing threats to broader public interests.

Third, Investment in Innovation and Professional Development. I have chartered the Commission's Technological Advisory Council (TAC) to explore specific opportunities where R&D activity beyond a single company might result in positive cybersecurity benefit for the entire industry. In collaboration with academia and communications technology stakeholders, we will identify incentives, impediments, and opportunities for security innovations in the market for communications hardware, firmware and software. We also must work with academia and NIST to evaluate the maturation of our nation's cybersecurity workforce. Cybersecurity professionals are among our nation's most talented, educated and dedicated workers. We seek to understand the current state of professional standards and accountability and with our partners understand where the FCC might positively contribute towards further professionalization of the workforce.

How will we measure success or failure of this new paradigm?

This is the toughest and most important question that our stakeholders have to answer.

We cannot continue on a path that lets individual networks put other networks, American businesses and consumers at risk.

We need to develop market accountability that doesn't currently exist.

Unlike financial risk, for which we have several centuries of quantified data on which to draw, quantitative cyber risk factors are relatively immature.

But that doesn't mean we just throw up our hands and give up.

I have directed FCC staff to work with our partners in the Federal government and the private sector to gather input on how to measure, assess and manage cyber risk in the communications sector.

Some common success factors are already emerging from that dialogue: First, companies conduct thorough inventories of their exposure to various cyber risks, internally and with their partners, Second, they conduct qualitative assessments of their management of those identified exposures to cyber risk. Third, they seek data from those qualitative assessments to develop quantitative metrics pertinent to their own internal needs. Fourth, they invest to close cyber readiness gaps making conscious, measured choices to mitigate risk.

In short: Identify the cyber risk universe, develop internal controls, assess implementation, and monitor effects. This sounds a lot like how enterprise risk management has always been done across all risks. Applying it to cyber risk would seem a no-brainer.

Companies must have the capacity to assure themselves, their shareholders and boards – and their nation – of the sufficiency of their own cyber risk management practices. These risk assessment approaches will undoubtedly differ company by company. But regardless of the specific approach a company might choose, it is crucial that companies develop methodologies that give them a meaningful understanding of their risk exposure and risk management posture that can be communicated internally and externally. That is what we are asking our stakeholders to do.

Once individual companies have an understanding of their own risk posture, then we can answer follow-on questions about the appropriate way to communicate this risk to business partners, customers, and the public.

We expect this to prompt a virtuous cycle of security, privacy and innovation, in which the market continually drives to improve these mutually reinforcing values. If so, ISPs will stand for Innovation, Security, and Privacy.

One last point: solving the technological challenges of cybersecurity is, for all its difficulties, the easy part. The hard part is changing behavior.

According to one study, 90 percent of breaches in a recent year could have been prevented with basic or intermediate security measures. People recognize that cybersecurity is a problem that must be addressed, but too few people are acting on this information – from consumers who may not know exactly why they need to update their passwords, to C-suite executives who don't yet fully grasp the threat that cyber attacks pose to their companies' viability, nor how they can match the risk with investment in cyber defenses**.**

We believe our work can help change behavior, and we expect that stakeholders will rise to this challenge.

The communications sector is at a critical juncture. We know there are threats to the communications networks upon which we all rely. We know those threats are growing. And we

have agreed that industry-based solutions are the right approach. The question is: will this approach work? We are not Pollyannas. We will implement this approach and measure results. It is those results that will tell us what, if any, next steps must be taken.