Remarks of FCC Chairman Tom Wheeler
As Prepared for Delivery
RSA Conference
April 21, 2015
San Francisco, CA

Thank you all for welcoming me. Special thanks to RSA and its leadership, Amit Yoran and Admiral Mike Brown. It's an honor to be part of such an impressive lineup of speakers. As an amateur historian who's written two books on the Civil War, I've always aspired to be part of a program that included Doris Kearns Goodwin. I just never imagined it would be at a cybersecurity conference in San Francisco.

I also appreciate that I get to speak to you on the same day as DHS Secretary Jeh Johnson. Cybersecurity is a collaborative effort, and our agencies are pursuing independent yet complementary initiatives to secure our communication networks – both public and private.

I come before you at a critical moment for the FCC's cybersecurity efforts. For more than a year, the Commission and key stakeholders have been working together to develop a strategy to enhance the security of our wired and wireless broadband networks. Last month, we all agreed on that plan. Now our focus shifts to implementation. Today, I want to visit about the keys to the successful execution of the Commission's cyber strategy, notably our plans to assure accountability and enhance information sharing by private sector stakeholders. I also want to look ahead to a key long-term challenge to successful cybersecurity: workforce development.

That cybersecurity is a national imperative is an irrefutable statement. Reliable and secure networks are the foundation of our digital economy and essential platforms for innovation, self-expression, and civic engagement. Moreover, these networks are vastly interdependent; localized attacks can have global implications, and the stakes continue to rise as our cyber adversaries become more sophisticated and devious in their methods. We will need bold and persistent leadership to get ahead and stay ahead of this challenge.

In a free-market democracy, that leadership must ultimately come from the private sector. Companies that rely on communications networks for their livelihood have the knowledge, expertise—and financial incentive—to get this right. Those that build, own, and operate these networks, and those that innovate at the edge of the networks, must work proactively and cooperatively to address shared risks. Companies need to "own" their cyber readiness.

This is the thinking behind the FCC's approach to cybersecurity. We believe the paradigm for cybersecurity is proactive and accountable self-governance within mutually agreed parameters. This isn't an ideological matter, but simply a logical conclusion. Things change so fast in the cyber world that prescriptive regulations could never hope to keep pace.

Cybersecurity requires sustained collaboration—between and among private companies, government agencies, and the public at large. Under the President's leadership, the National Institute for Standards and Technology (NIST) led development of a business-driven, proactive framework for voluntary cyber risk management. This is a tool designed for companies of all sizes that operate in diverse sectors of the economy and in a variety of dynamic risk environments.

The NIST Framework is the essential starting point for any collaborative engagement on cybersecurity. It provides a common language for identifying, assessing, and responding to cyber risks and threats. The Framework also represents a substantial commitment from the private sector.

We see the FCC's role as building on the NIST Framework in the context of our responsibility to promote the reliability and resiliency of the communications networks themselves. Businesses and consumers place their faith in these networks everyday. Any comprehensive effort to address cybersecurity must include securing these essential conduits of economic and social activity.

The FCC has a proven track record of partnership with the communications sector to fortify our nation's networks. FCC advisory bodies have, over the years, produced a rich repository of analyses and best practices to guide the evolution of the network industry. More recently, these have included measures aimed at securing core networks against inherent vulnerabilities, such as IP-route hijacking and address spoofing. The FCC has actively engaged the industry in confronting these persistent disruptions to communications. This has included working one-on-one with companies to assess progress and overcome barriers to improvement.

Last year, we asked the Communications Security, Reliability and Interoperability Council (CSRIC), our advisory committee on these issues, to develop and recommend voluntary mechanisms by which the communications industry can improve their management of cyber risks and clarify accountability within the corporate structure. They broke the NIST framework open, analyzed each of the 98 sub-categories for applicability to communications providers, and developed implementation guides for each subsector, plus tailored steps for small- and medium-sized businesses.

While this design work was important, the most vital work centered around ensuring accountability. CSRIC developed a range of activities intended to provide transparent assurances to the FCC, to DHS, to industry, and to consumers. These visible assurances should provide confidence that companies throughout the sector are actually taking effective steps to manage cyber risk. Over 100 private sector companies and industry associations representing thousands more participated in this endeavor. They came from all corners of the industry, offering the unique perspectives of ISPs, wireless carriers, broadcasters, and other industry participants. Public interest groups and federal, state, and local government agencies also played a crucial role.

After an intense year, CSRIC voted to approve its management and accountability procedures last month. As we engaged with industry representatives and reviewed the information in the CSRIC report, we were guided by two questions: First, does the report convey a real commitment from the industry to a level of accountability that meets the FCC's expectations and that serves the public interest? Second, how will these commitments translate into meaningful, long-term action and results, when the press conferences are long past?

On the first question about industry commitment, I am pleased to say that CSRIC's final report contains a compelling set of recommendations for cyber risk management throughout all segments of the communications sector. It articulates a comprehensive approach, rooted in the NIST Framework, while also taking note of the unique challenges that face providers of various kinds. Most significantly, the report calls upon industry stakeholders to undertake a significant assurance process.

CSRIC's core proposal is that members of the communications sector volunteer to participate in individualized, face-to-face meetings with the FCC to discuss each company's cyber risk management priorities, methods to address them, and the effectiveness of these methods. These meetings would be guided by the NIST Framework and occur at periodic intervals.

How will this assurance process work in practice? The FCC and its industry partners are still working out the details, but we already know a few fundamental points. First, these assurance meetings will not be depositions. We do not envision an adversarial process in which corporate officials are cross-examined in an attempt to draw out embarrassing admissions about security lapses. On the other hand, there needs to be more than glossy PowerPoints and prepared remarks read off a script. The sweet spot is a process that is open, honest, and interactive, with the parties working as partners in addressing a matter of national concern. Both groups should benefit from the exchange, as the FCC staff gain better appreciation for the challenges and the range of approaches applied against these challenges.

Of course, the frankness and candor of these exchanges will depend largely on whether companies feel that they can trust in the process. There must be adequate safeguards in place to ensure that any sensitive information shared during these meetings is protected from public disclosure. Companies must also be relieved of any suspicion that information shared in these meetings will be used to generate regulatory proposals. That is not their purpose.

So just what is our expectation for these meetings? The answer is that we expect a thorough demonstration that a company’s cyber risk management program is effective. Using the risk framework drives companies to consider their readiness not just in stopping attacks, but in each of the Identify, Protect, Detect, Respond, and Recover phases critical to minimizing the impact of a malicious attack. The risk framework doesn't stand alone, companies need to have threat intelligence, they need to address supply chain risk and insider threats among other areas, but the Risk Management Framework provides a great foundation from which to see the gaps and organize effective mitigation.

To be clear, the FCC's role is not to second-guess a company's business judgment or to micromanage its implementation of the NIST Framework. We simply care about one question: Does it work? Are companies regularly and systematically assessing threats and vulnerabilities, analyzing their capacity to address risk effectively, and mitigating risk through people, processes, and systems?

Of course, the business of assessing and measuring the effectiveness of a company's practices is not that simple. There needs to be a common understanding of the indicators of success. What does a cyber-secure network look like? CSRIC's report emphasizes the importance of network availability – that is, the ability of networks to continue delivering service in the face of an attack. Further work needs to be done to develop quantitative metrics around this concept, and related concepts such as confidentiality and integrity of network services and information flows. There is an old management axiom: if you can measure it, you can manage it. Never has that been more important than in cyber.

Without a doubt, CSRIC has outlined a process with real promise, and they deserve high marks for getting us to this point. But because there is a lot of material in their report to consider, and many parties outside the CSRIC process are likely to have their own ideas to contribute, we've put CSRIC's report out for public comment. I encourage you to read the report if you haven't already and give us your thoughts.

When fully developed and properly implemented, I believe that CSRIC's assurance model will provide much-needed accountability for network security, while avoiding top-down prescriptive regulation of industry practices. A cooperative and collaborative approach is the FCC's preferred means of engagement. I have every reason to be confident the industry will live up to its commitments and deliver meaningful action. But the hard work has only begun and our review of these next steps will be guided by the fact that cybersecurity is a national imperative.

As we move into the implementation phase of this roadmap, perhaps the biggest challenge we must tackle is improved information sharing. This is a common challenge and there must be mechanisms in place to enable the flow of real-time information among relevant stakeholders, so that they can work together in real-time. The highest need for this collaboration is in the private sector, in particular among the operators of our nation's interdependent networks and their corporate customers.

Let's pause here to emphasize the word "interdependent." The simple fact is that a network is a network because it connects with other networks.

Now, concerns have been raised in the past about the logistics and the legality of communications networks sharing cyber threat information with their competitors. But in an interdependent world, such sharing is essential. My view is that there are no insurmountable barriers to making this work, and the public interest demands nothing less. Recent guidance from the Justice Department and Federal Trade Commission suggests that antitrust concerns should be minimal to non-existent if the sharing is framed correctly. If there are other lingering anxieties, let's get them out in the open and address them together. If there's a will, there's a way.

In our effort to improve the flow of real-time cyber threat information, the FCC works in close partnership with the Department of Homeland Security, which takes the lead in information sharing within government. Most recently, the FCC has established a partnership with DHS that provides the FCC access to the NCCIC (National Cybersecurity and Communications Integration Center), which is the single authoritative focal point for the sharing of cyber threat indicators. The FCC has a mature outage reporting mechanism in place with the communications sector, which we share with DHS and have proposed to share with the states, and it is our goal to avoid duplicative reporting requirements and to ensure that the interface with industry is clearly outlined.

As the nation's "network" agency, the FCC has a unique role to play in any discussion about network security. It's part of our statutory charge to protect the safety of communications for the benefit of the public. Specifically, think about the reliability and resilience of networks to complete a 911 call. Traditionally, the FCC has ensured the overall reliability of communications networks through a two-pronged approach: voluntary industry best practices, coupled with mandatory reporting of significant network outages. This approach has resulted in the world's best emergency call network, through continual improvements in the state of network reliability.

The time has come to think about whether and how cybersecurity fits into this framework. Though cyber attacks may not cause network "outages" in the traditional sense of the term, the most severe attacks can cripple service for vast swaths of users. When we talk about the security of our networks we must also think about public safety. Reporting on these events may helpfully complement other methods the FCC uses to gather information about the cyber health of our communications networks.

We are also continuing to examine how the concept of cybersecurity intersects with other aspects of the FCC's statutory mission. For instance, the FCC has explicit responsibilities to protect the privacy of data that communications providers collect from their customers in the everyday course of business. Consumers have a right to expect that this information will be protected from disclosure. Failure to do so can have a chilling effect on free expression and the virtuous cycle of network investment and innovation.

Let me close by touching briefly on a critical long-term key to combating online threats: the cybersecurity workforce. Simply put, the largest single investment in an effective cyber program is in its people.

To assure we have a workforce capable of defending against cyber threats, it will take a shift in our thinking. Specifically, the "people" element of cyber has to become a bigger part of our corporate thinking. We need to bridge the gaps between cyber IT and HR, and engage with the institutions that educate and train the next generation of cyber-capable workers. The Defense Department and the intelligence community recognized this several years ago and took proactive steps to jumpstart the pipeline of new cyber professionals for its own needs. We need a similar commitment to meeting the talent needs of private industry, as well as state and local government.

As the cyber threat landscape changes, so too must the practice of cybersecurity and its relation to other disciplines. We need to make sure we are investing sufficiently in the next generation of cyber engineers, but also in cyber lawyers, auditors, and business leaders. Cyber risk managers may very well be the next interdisciplinary cyber specialty on everyone's "to hire" list.

NIST has done great work in this area, and the FCC is committed to leveraging that work and promoting the development of qualified cyber professionals to meet the growing need for workers to secure our critical communications infrastructure in the public and private sectors. Soon we will be considering new assignments for CSRIC, and this a topic that I will expect them to tackle. I also expect that workforce issues will play a meaningful role in the work of an FCC task force that is examining the emerging challenges that face 911 call centers.

We need people who can interpret and translate the language of cyber risk at all levels of the business and government, up to the C-Suite, as well as communicate with investors and regulators. Cybersecurity cannot be imposed from above; it must be built into institutions and enterprises from the bottom up.

A culture of cyber responsibility and professionalism cannot be developed overnight, nor can the FCC do this alone. Cybersecurity needs to become part of the lexicon, part of the way we do business. Today, we have discussed three of the highest priorities at the FCC: implementation of new risk-based cyber programs across the commercial sector; greatly enhanced information sharing about cyber threats between companies and the government, and an educated and trained cyber workforce ready to meet the demand inherent in the technology transitions occurring across the communications landscape.

So, I'll conclude by speaking directly to those who run the companies that run our networks. These plans will only succeed if there are real commitments to cybersecurity from those who occupy the loftiest corporate perches. As a former public company board member I know that things only happen when the C-Suite takes ownership of an issue. Our corporate leaders must also be cybersecurity leaders by making it clear throughout the organization that cybersecurity is an institutional priority. We are all in this together. And by "we" I don't just mean the networks and the FCC … I mean all Americans. We must get this right. Working together, we will get this right.

Thank you.