Remarks for Admiral David Simpson
WTA – Advocates for Rural Broadband Spring Meeting
Cybersecurity Panel

May 5th, 2015
10:00 - 11:30 a.m.
Hyatt Regency, Indian Wells, CA

Thank you all for welcoming me. It is a privilege to address WTA-Advocates for Rural Broadband and its members. We appreciate the leadership role you have taken on so many important issues for small and rural carriers, and the key contributions you have made in many of the Commissions proceedings.

As you know, one of the major responsibilities the FCC has is ensuring that our country's communications networks function reliably and securely. Strong cybersecurity policies and protections are crucial to maintaining that reliability and security. Cybersecurity isn't just about having good anti-virus software and changing your passwords, that is what we call "cyber hygiene". Cybersecurity is a long-term risk management approach that should be baked into all levels of strategic thinking.

We have been working to ensure that all sectors of the communications arena are equipped to protect their networks and businesses from cyber attacks. This work needs the participation and cooperation of all parties: government and industry,

public and private, large and small, groups and individuals. Our cybersecurity efforts at the FCC have been aimed at including all stakeholders in this effort. We have taken a collaborative approach to cybersecurity, working in partnership with private-sector stakeholders through a federal advisory committee, the Communications Security, Reliability and Interoperability Council (otherwise known as "CSRIC"). Through CSRIC we have worked closely with members of the communications industry because we know that a proactive industry posture that is measurable and accountable lies at the heart of the communications security and reliability strategies we need to maintain the integrity of our networks. We have to do it together, in a coordinated approach that draws on every stakeholder's particular strengths.

At a public meeting in March, CSRIC IV unanimously voted to recommend to the FCC voluntary mechanisms to implement cyber risk management practices based on the 2014 NIST Cybersecurity Framework to the communications sector. The federal government and private industry in the U.S. have both identified the NIST Framework as the best mechanism for tackling cybersecurity. It can be utilized to update or develop cyber risk management programs and is adaptable to an entity's unique circumstances.

The CSRIC effort encompassed all five communications industry segments – wireline, wireless, satellite, cable, and broadcast. These segments were able to prioritize the risk factors presented in the NIST Framework of the most important to them. Each industry segment further defined their "core network" and "critical infrastructure and services" and focused on providing a roadmap for their industry to align their specific operations to that of the NIST Cybersecurity Framework. In addition, a Small and Medium Business Group specifically focused on how to apply the NIST Cybersecurity Framework to small and medium sized operations, while respecting challenges related to their size and limited resources, also contributed to the effort. All of these groups worked together to create the foundation of a new paradigm, where industry implements measurable and accountable voluntary mechanisms that potentially can address fast-changing technology-based issues better than prescriptive regulation. There is no truer test of this new paradigm than cybersecurity.

The FCC knows that smaller carriers often have fewer resources available to them and Section 9.9 of the CSRIC Report offers guidance designed specifically for smaller carriers. This section provides smaller carriers with a formalized and structured risk-management approach to address cybersecurity, applying the NIST Framework based upon their unique needs and operational environment. The SMB

group evaluated the 98 subcategories in the NIST Framework and selected a high-priority subset of 37 for smaller carriers to use as a starting point in their assessment. The high-priority subset can be found in Appendix II. It lays out three basic questions for smaller carriers: What do you need to protect? Who has the responsibility for a given task? and, How will you protect your core network and critical infrastructure and services (i.e. develop plans for identification, prevention, recovery, and continual improvement)?

The day after CSRIC adopted the recommendations, the FCC put them out for public comment. We want to hear the opinion of folks in the sector and in related industries as to how they view the recommendations and whether the voluntary mechanisms proposed provide a sufficient basis for the FCC to conclude that all industry segments are effectively managing cyber risk. The comment period is open through May 29th (with replies requested by June 6), and we hope to hear from as broad a cross-section of the U.S. as possible, to help us as we look toward our next task: implementation and certification.

As we shift our focus to implementation, I want to discuss what is necessary for the successful execution of the Commission's cyber strategy, notably our plans to assure accountability and enhance information sharing by private sector

stakeholders. 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. However, we still need to ensure that these commitments will lead to meaningful, long-term action and results.

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? We are still working out the details, with input and ideas from industry, and we certainly need to hear more from small and medium sized carriers, but we have already identified a few fundamental points. First, these assurance meetings will not be depositions. We do not envision an adversarial process in which owners and officials are cross-examined in an attempt to draw out embarrassing admissions about security lapses. On the other hand, we need to hear more than prepared remarks read off a script

about general processes and procedures. The ideal that we envision 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, as I stated earlier, we've put CSRIC's report out for public comment. I encourage you all to read the report if you haven't already and give us your thoughts. We need to hear from small and medium sized businesses in particular, to figure out the most effective and efficient way to meet with all of you to ensure that your company's cyber risk management program is effective but not to place too great a burden on anyone as part of that process.

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 the cybersecurity 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 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, I 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 talking directly to you as small and medium sized carriers, these plans will only succeed if there are real commitments to cybersecurity from those who own all parts of our communications networks. Our smaller carriers must become cybersecurity leaders by making it clear throughout the country, even in our most rural and remote areas, that cybersecurity is a national priority that affects us all. 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, sharing information, and taking well-coordinated measures to secure and restore critical communications capabilities will ensure the continued availability of these vital links for our society. I now look forward to your questions.