Remarks of David Simpson, Rear Admiral (Ret.)
Chief, Public Safety and Homeland Security Bureau
Federal Communications Commission

Before WTA's Cybersecurity Panel
Las Vegas, NV
April 8, 2014

-As Prepared for Delivery-

Good afternoon. I'd like to thank you for having me here today. This is my first time speaking with the WTA and I want you to know that I understand and appreciate the valuable work that you do and the challenges you face bringing up-to-date communications to some of the most isolated and underserved communities in our Nation. I find it truly remarkable that companies like ATC Communications in Albion, Idaho and ToledoTel in Toledo, Washington, founded as family businesses a century ago, continue to provide members of their communities with modern communications services in this climate of breakneck technological advances. For much of my career, I've worked to create, sustain, and defend networks of similar size in remote terrain and under adverse conditions – and I have every respect for the valuable role you play in your communities.

Advancements in communications have bestowed so many benefits. The world is now essentially delivered to your door through broadband connections, helping to match needs and resources. And there is great security knowing that emergency assistance is simply a 911 call away. Consumers can enjoy the benefits of commerce and medical services even if they live many miles from the nearest mall or hospital. But with brilliant innovation comes a new set of challenges: ensuring that future IP networks are reliable, resilient, and secure, and ensuring that public safety resources are accessible in times of crisis.

A core mission of the FCC is to ensure that the Nation's communications infrastructure is secure and reliable. We take this seriously and recognize that the responsibility is universal, and it extends to Americans in every part of the country, however remote. Private sector companies own and control the vast majority of our Nation's networks and share the same commitment towards public safety. As we look forward, the challenge of keeping networks reliable and secure is too important and increasingly sophisticated for organizations to "go it alone." Effective information sharing is a critical component of cyber defense. We must work together between companies within a given sector, between sectors, and with cyber-capable government organizations.

The FCC has long taken this approach, working in partnership with private sector stakeholders through our federal advisory committees, the Communications Security, Reliability and Interoperability Council (CSRIC) and the Technical Advisory Committee (TAC). Representatives from all facets of the communications landscape – including large, small, and rural communications companies; academia; public interest groups; government partners; and other stakeholders – contribute their time, expertise, and unique perspectives to tackle some of the most challenging communications issues facing us today.

Chairman Wheeler has spoken frequently about his intention to increase the FCC's commitment to these private–public cybersecurity efforts. And the Cybersecurity Framework recently released by the National Institute of Standards and Technology (NIST) also follows this model, calling for voluntary public and private sector coordination.

Cybersecurity

In 2011, the CSRIC adopted recommendations for voluntary measures to mitigate some of the most difficult Internet security problems: inter-domain routing security, Domain Name System (DNS) security, and botnet threats that affect consumers and enterprises in the form of DDoS attacks. But that was just the beginning. The FCC actively participated in the drafting of the NIST Cybersecurity Framework and now continues to support its adoption by working with the Department of Homeland Security (DHS) in its efforts to implement the Framework. And we continue the work of the CSRIC.

The NIST Cybersecurity Framework is designed to provide organizations –regardless of size, scope or cybersecurity sophistication – with a structure to organize and manage cybersecurity risk in their infrastructure. In a non-switched, all IP world, this will be not only a valuable security measure, but also an important efficiency measure easing demands for manpower and expertise that smaller companies might incur in trying to reduce cyber risk.

The DHS website (http://www.dhs.gov/using-cybersecurity-framework) provides detailed guidance for companies seeking to implement the Framework. It offers a Cyber Resilience Review, a no–cost, voluntary, non–technical assessment to evaluate an organization's operational resilience and cybersecurity practices, as well as other guidance for assessing your organization's specific vulnerabilities. The assessment will lead to recommendations about how to fix cybersecurity gaps, as well as suggestions on how to tackle future cybersecurity threats. The website also provides many resources to support alerting and sharing of current cyber threat information, and can direct you to extensive cyber training resources. Finally, DHS has located regional DHS Cyber Security Advisors and Protective Security Advisors who can offer immediate and sustained assistance for critical infrastructure cybersecurity needs.

The FCC has formed a CSRIC working group to optimize the Framework for communications providers. Specifically, CSRIC's Working Group 4, which just launched in March, is working to update an existing set of cybersecurity best practices, harmonize them with the NIST Framework, and provide for business-driven cyber risk management based on the Framework. This work will help communications providers to operationalize the Framework by creating a "Rosetta stone" that will help translate best practices into effective measures that reduce risk in more measurable ways, thereby improving a providers' cybersecurity posture and facilitating better communication of needs and expectations internally and with external stakeholders.

These best practices can be of particular assistance to small to mid–sized telecom companies. We realize you may not have the resources or expertise to formulate detailed cyber plans on your own. The CSRIC's work to create generic implementation templates will be

complete in March 2015. In the interim, you might take a look at the FCC Small Biz Cyber Planner, available on the FCC website. It provides a customized cyber plan to address small- to medium-sized businesses' most prominent cybersecurity risks.

CSRIC Working Group 5 will examine and make recommendations to the FCC regarding network-level best practices and other measures to mitigate the effects of DDoS attacks from large data centers and hosting sites. In addition, CSRIC Working Group 6 will identify and plan for long-term remedies to Domain Name Security vulnerabilities, including practical implementation plans to better secure the Domain Name System infrastructure.

The FCC's TAC will also focus on cybersecurity this year. It will examine opportunities to engage early in the development of hardware and software to incorporate features that can greatly improve enterprise–wide defensive capabilities. This is an area small providers can benefit from. Help us understand your defensive cost drivers and barriers to effective defense.

Without access to real–time cyber threat information, organizations are left helpless in the face of a cyber–attack – and quite frankly, the current system is not sufficient. This applies both for small-scale and nationwide operations. Part 4 of the Commission's rules requires communications providers to report outages of a certain magnitude to the Commission through our Network Outage Reporting System (NORS). Over a year ago, VoIP outages were added to the collection. The FCC also has a Disaster Information Reporting System (DIRS) that allows communications providers to voluntarily report outages and request assistance with getting communications up and running as quickly as possible after a disaster. Broadband providers are included in DIRS. Broadband is not currently covered under NORS, but as legacy switched services migrate to broadband, we will need to ensure that reporting continues to provide detail on outages impacting public safety.

Technology Transitions Order–IP Trials for Rural Broadband

Another current focus of the Commission is easing the transition to an all–IP environment. The Technology Transitions Order, adopted in January, calls for tests of real–world applications, as well as targeted experiments and cooperative research as part of the path to "sunset" legacy switched service. Included in the Order is a call for rural broadband experiments to specifically ease the transition to an "all IP" world in remote communities. We invite proposals for bringing advanced services to rural America with support from the Connect America fund. We intend to focus on building robust last-mile broadband in high-cost areas lacking broadband Internet access. The Order also seeks further comment on budget, selection criteria, and other implementation issues, such as whether to modify approaches in rate–of–return areas.

The experiments are intended to gather information about interest in extending fiber, characteristics of areas where providers would prefer to deploy wireless, and what types of wireless offerings residential customers would find acceptable, the impact on anchor community institutions, and how to to work cooperatively with States, localities, and Tribal governments. It will be essential that service provided through this mechanism is secure. This may be a challenge for smaller providers, but it is just as important for rural consumers that their service is

reasonably protected as it is for consumers with service from large carriers. If the sustainment cost for cybersecurity is an inhibitor to effective rural deployment, it would be important for the Commission to hear this.

Thus far, we have about 1000 expressions of interest filed. Comments on open issues were due March 31st and replies are due April 14th. After reviewing the record, the FCC will adopt budget and criteria for selecting experiments. Finally, through a second order we will solicit formal project proposals. We expect to select a small number of projects later in 2014.

911 Reliability Proceeding

Before I sit down and answer your questions, I want to briefly update you on some of the issues affecting 911 in which the Commission is actively engaged. The first is 911 reliability. The FCC's historical approach to 911 reliability has been to promote voluntary development and implementation of industry–driven best practices and to measure implementation of best practices through mandatory Part 4 outage reporting.

In December 2013, the Commission adopted a Report and Order requiring 911 service providers to take *reasonable measures* in three key areas to provide reliable service, as evidenced by an annual certification. Covered 911 service providers must certify compliance with specified best practices or reasonable alternative measures to mitigate the risk of failure in the areas of (1) critical 911 circuit diversity, (2) central office backup power, and (3) diverse network monitoring.

This certification approach will allow the FCC to hold service providers accountable for reliable 911 service, while offering flexibility in how they design and operate their networks in different parts of the country, including rural areas. The Report and Order also amended existing FCC rules to ensure that Public Safety Answering Points (PSAPs) receive more timely and specific notifications of 911 outages.

WTA filed comments in this proceeding asserting that "[r]ather than adopting unnecessary new nationwide 911 service rules applicable to all carriers, the Commission would be better advised either to exempt RLECs and other small rural entities from the proposed new rules or, in the alternative, to use its informal complaint process to identify and resolve the relatively few instances where PSAPs may be unhappy with their 911 service."

We understand your concern that best practices developed by large companies with nationwide footprints are not always scalable or cost effective for RLECs. Although there is no formal waiver or exemption for rural providers, the certification was designed so that many of the requirements (e.g. circuit auditing and tagging, diverse network monitoring) will not apply unless a 911 service provider operates a selective router or ALI/ANI database.

Portions of these new rules took effect February 18. 911 service providers are now under an enforceable obligation to take reasonable measures to provide reliable service in each of the three areas covered by the certification. This increased accountability for resilient capabilities is

appropriate and should help all Americans have greater confidence that when they have an emergency their 911 call will go through.

The annual certification and revised PSAP outage notification requirements involve a collection of information that must be approved by the Office of Management and Budget (OMB), and this will take several more months. The FCC will issue a public notice once effective dates for these rules are established.

Finally, the FCC continues its work on a range of text-to-911 issues, including the implementation of text-to-911 service for over-the-top text messaging providers, the provision of location information with text messages to 911, roaming, and PSAP implementation. We are optimistic that the parties to the carrier agreement will fulfill their commitments in May of this year. We will next turn our attention towards ensuring this capability becomes a norm across the nation.

Conclusion

I would like to thank you again for the opportunity to speak with you today. The FCC remains committed to ensuring that all Americans have access to the marvels that are modern-day communications and the best protections available to allow communications to be enjoyed on a reliable basis without fear of theft, intrusion, or failure.

I look forward to answering any questions you may have and to hearing your thoughts.

-#-