Remarks of Chairman Tom Wheeler

NSTAC Closed Session
November 19, 2014

I. Introduction

Thank you for having me here today.

When I was last here, I had barely been in this job a few weeks. What an eventful year we've had since then! Today, I'd like to speak with you about what I expect will be significant steps forward in private sector leadership on cyber security in the communications sector.

The FCC's fundamental responsibility is to ensure the security and reliability of our nation's communications functions. That's particularly true for the "can't fail" public safety communications imperatives on which lives depend. We must ensure that 911 calls go through, that emergency alerts are credible, and that the core network communications infrastructure that we all count on is reliable.

The challenge we face is this: how to challenge the marketplace to respond to these realities in an all-Internet Protocol communications world, and what to do if that isn't sufficient. One example of this was a recent shocking outage of 911 service across multiple states in which a software glitch in one server in Colorado disrupted this crucial emergency service for over 11 million people in states ranging from the Pacific Northwest to the Carolinas. As dismaying as this particular outage was, my concerns are exacerbated when certain service providers rationalize these failures with "stuff happens" excuses rather than developing solutions to keep 911 in service even when "stuff" does happen. In response, we will on Friday consider a Notice of Proposed Rulemaking that would clarify the accountability and proactive responsibilities that providers and other stakeholders must bring to this new 911 environment to ensure that calls for help always go through.

This "sunny day" multi-state 911 outage–caused not by a storm or natural disaster but by a software glitch with consequences that reached across our continent–is a harbinger of future challenges that apply more broadly in our ongoing transition to Internet Protocol-based communications. In an environment where a bad guy with a keyboard anywhere on the globe is a potential threat, the private companies that operate these services are our nation's first line of defense.

America's infrastructure companies must step up. ***Proactively***. As if their business depends on it… because it does.

If critically-positioned companies just comply ***reactively*** with a regime of prescribed mandatory requirements then our networks will always be a step behind. This is particularly true vis-à-vis aggressors. These threats move faster than a notice-and-comment rulemaking process. We need

a solution that allows companies to move faster as well, both for their own good, and for the good of the nation.

A proactive industry posture is at the heart of a cyber risk management strategy in our sector that is business-driven, measurable, and accountable. Moreover, we have challenged the stakeholders in the communications sector to develop this approach themselves. We expect their solution to be more flexible and dynamic than traditional regulation, and demonstrably more effective than blindly trusting the market to meet consumers' security needs.

This new paradigm approach is the opposite of checklist-oriented compliance. Let me be crystal clear on this point: I do ***not*** believe that a compliance checklist is the right answer for cyber risk management. Rather, I want companies to develop a dynamic strategy that can be both more effective and more adaptive than a traditional prescriptive regulatory approach.

II. Importance of Cross-Sector Coordination

One of the most salient truths about our nation's networks today is that they are deeply interconnected. As a result, a vulnerability in one company's network can potentially reach across the nation's broader web of networks. Because the telecom sector links every aspect of our economy, I asked our team early on to collaborate with all our key interagency partners, and especially those in sectors that depend on secure, reliable communications.

Admiral David Simpson, our Public Safety and Homeland Security Bureau Chief, pitched the idea of convening a formal group of regulators to coordinate on these issues across sectors, and we were pleased to learn that the Nuclear Regulatory Commission had already started to plan just such an initiative.

Since then, NRC staff have partnered closely and productively with FCC staff and those of other agencies. In October, we launched the Cybersecurity Forum for Independent and Executive Branch Agencies in order to better coordinate and streamline our activities.

This is crucially important work, because we all know we cannot address these cyber threats in sector-by-sector stovepipes. We have to approach our cyber challenges in a way that builds on our various authorities and activities.

Admiral Simpson, who started his Navy career as a propulsion engineer, calls this "adding torque." This Forum is a vehicle for adding torque, particularly where crucial interdependencies exist between our companies and sectors. We expect the Forum to help knit together cyber defenses of the companies across our various sectors – all of which are dependent on each other, and all of which can assist each other.

But, as the Admiral has also reminded me, torque without RPM doesn't get you there. And in this equation, information sharing is the RPM. That means sharing situational awareness and notices regarding threats and vulnerabilities. Our companies are our country's eyes and ears. We need them to take the lead in information sharing in three different ways:

- First, among one another within their sector.

- Second, between companies in different sectors.

- And third, between the companies and the government.

As some of you may know, the FCC plays a convening and information exchange role to help the communications sector organize to get through hurricane season every year. With common sense examples like that in mind, we need to help companies develop cyber information sharing partnerships that are dynamic enough to keep up with these ever-changing threats.

Information sharing is an essential element of predictive, proactive defense against a high-end adversary. We are seeking to improve that sharing by identifying and addressing legal or practical barriers, and facilitating regular communication across all our partners. On that last point, this afternoon's discussion led by Secretary Moniz will no doubt illuminate our understanding of the challenges between the communications sector and the electric power sector.

These are hard questions, but it is very important that we work together, channeling private sector leadership and expertise, to develop solutions.

III. Measurable, Accountable Risk Management

The second core element of our work in the new paradigm is helping businesses develop the tools to manage cyber risk as a core business function.

The NIST Cybersecurity Framework is a very valuable tool in this regard, because it is a risk management approach rather than a compliance checklist. It recognizes that cyber risks are here to stay, that there's no checklist that can fully protect your networks, and that companies need to address those risks as a basic part of doing business.

In this sense, cyber risk is like financial risk – it's just harder to measure because we have not done it before.

We as regulators must help clarify this new risk reality in terms that boards, executives, investors, and insurers can understand. It is a simple equation involving traditional measurements such as cost/benefit, return on investment, and protection against loss. Yes, cyber is a national security problem, but it is also a business problem and business leaders must embrace real measurement and real accountability. Not only does this require investment in cybersecurity, but also a commitment to run cyber defense operations based on hard facts and analysis, with market rewards for good performance. To help them, we regulators need to ask questions like:

- What specific measurements would be useful in these internal assessments of cyber risk, including how best to evaluate the effectiveness of cyber defenses? Can such tools help businesses to "price" their risk exposure and make cyber investment decisions?

- What do boards and CEOs need to know about their companies' cyber risk exposure and how those risks are being addressed?

- What assurances should companies offer externally to business partners, investors, customers, and government authorities regarding the effectiveness of their cyber risk management and the reliability, resiliency, integrity, and security of their core services?

The Communications Security, Reliability, and Interoperability Council, or CSRIC, is the FCC's advisory committee that is applying the NIST Framework in the communications sector. We have asked CSRIC to address these questions in implementing a measurable, accountable, business-driven approach.

Specifically, we have asked CSRIC to develop, and I quote:

> "voluntary mechanisms to provide macro-level assurance to the FCC and the public that communications providers are taking the necessary corporate and operational measures to manage cybersecurity risks across the enterprise."

What do we have in mind for these assurances? Again I'll quote from our charge to CSRIC:

> "These assurances: (1) can be tailored by individual companies to suit their unique needs, characteristics, and risks (i.e., not one-size-fits-all), (2) are based on meaningful indicators of successful… cyber risk management… , and (3) allow for meaningful assessments both internally… and externally."

There are over 100 cybersecurity experts from communications companies large and small that are working on this landmark initiative, and CSRIC will deliver its recommendations this coming March. We are pleased with the progress the group appears to be making and the seriousness with which they are working on these hard questions. The bottom line, right now, is that we expect CSRIC and its members to deliver a new paradigm of voluntary mechanisms and meaningful assurances about the effectiveness of risk management measures.

Meaningful, measurable, accountable assurances, driven primarily by the business needs of the companies in the communications sector – that's what we're looking for.

With industry hard at work through the CSRIC to develop meaningful cybersecurity recommendations, we will soon have to turn our attention to implementation: that is, are companies actively and effectively implementing those recommendations? To that end, we are looking into the possible benefits that might accrue to companies who step up voluntarily into this new paradigm and do the right thing for their businesses and their country.

Those companies will be doing right by their businesses, the broader communications sector, and the nation as a whole. They will be sharing the problems and cyber challenges they are facing, with an eye to solutions that benefit that company's bottom line along with the whole communications sector's performance and prosperity. When we do this right, an attack on one company actually serves to improve everybody's defenses.

It only makes sense that companies that step up should get some form of "credit" or incentive for their actions. As CSRIC completes its work on the home stretch, I have invited them to give us creative recommendations about what that might mean in practice and in law. This is a complicated endeavor. But it's a promising element of the overall effort, and we are seeking innovative solutions.

On the other hand, what about companies that decide not to step up to use this business-driven new paradigm that the communications companies themselves created? Well, I don't know why companies wouldn't opt in to their own industry-created approach, but if they choose not to do so, we will have to find other ways for them to communicate their cyber readiness.

IV. Conclusion

I have said many times, both to my staff and to the public, that the FCC will never be as fast or as innovative as the Internet. The solutions to counter aggressive, thinking adversaries will come from the front lines – from the network operators and service providers that are under attack every day. And it is our near-term task to help develop a structure that provides us all with the right environment to help them succeed and, in doing so, enhances our nation's security.

We want the companies themselves to take the lead, and we are confident that they will.

Businesses need ever-changing, ever-ready dynamic risk management, not a check-the-block list of compliance, to address the cyber threats that their companies and our country face.

We at the Commission stand ready to do our part.