TESTIMONY OF DIANE RINALDO

ASSISTANT SECRETARY FOR COMMUNICATIONS AND INFORMATION (ACTING)

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

U.S. DEPARTMENT OF COMMERCE

HEARING ON SUPPLY CHAIN SECURITY, GLOBAL COMPETITIVENESS, AND 5G

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

October 31, 2019

Chairman Johnson, Ranking Member Peters, and Members of the Committee:

Thank you for this opportunity to testify today on Supply Chain Security, Global Competitiveness, and 5G.

The National Telecommunications and Information Administration (NTIA) in the Department of Commerce is responsible for advising the President on telecommunications and information policy. NTIA's programs and policymaking focus on a broad range of issues that include spectrum management and availability, broadband connectivity, and the growth and stability of the Internet. NTIA also is the agency charged with oversight of FirstNet, the independent authority within NTIA that is tasked with ensuring the development, building, and operating of the nationwide broadband network that equips first responders with essential digital tools that help save lives and protect U.S. communities.

During a time when an ever-changing landscape of services, technologies, and global industries are seeking to shape the development and deployment of 5G networks, NTIA collaborates with other Commerce bureaus and Executive Branch agencies to develop and advocate for domestic and international policies that preserve the open Internet and advance key U.S. interests. NTIA coordinates Executive Branch communications activities and represents the Administration's policies before the Federal Communications Commission (FCC).

The Nation's telecommunications infrastructure is the physical medium through which all Internet traffic flows. It underpins the foundation of our digital economy. NTIA's role is to foster national safety and security, economic prosperity, and the delivery of critical public services through telecommunications. In this capacity, NTIA is involved in numerous policy issues that affect the security of critical elements of our Nation's telecommunications infrastructure.

Our support includes working with our interagency partners to enhance the security of our Nation's telecommunications supply chain, advocating the United States' longstanding policy against data localization regimes, and participating in Executive Branch reviews of applications before the FCC that involve transactions with a significant foreign ownership component. We also are assisting the Secretary of Commerce, as needed, on the implementation of the Executive Order on Securing the Information and Communications Technology and Services Supply Chain.

Managing U.S. Spectrum Resources

The United States is dependent on reliable access to the finite resource that is radiofrequency spectrum. The Federal government is the most sophisticated consumer of spectrum in the world. Our armed forces, law enforcement agencies, scientists, and engineers all rely on spectrum to successfully serve the public. By protecting critical spectrum resources, we ensure that our military remains strong and our scientific understanding remains second to none.

At the same time, our technology industries lead the world in putting spectrum to use in innovative ways that bring massive economic and societal benefits to Americans. These range from powering the connectivity of the smart devices in our hands to the satellites circling in our skies.

In our competitive world, our country does not have the luxury of pursuing only some of our national priorities. We must pursue and achieve all of them, which will require the ingenuity and close coordination between NTIA and all of our federal partners as well as the private-sector.

As with any critical resource, access to spectrum must be managed efficiently and effectively in order to provide additional spectrum for wireless 5G spectrum access while ensuring federal agencies have sufficient spectrum to complete their missions. As management of spectrum licenses or authorizations becomes more automated and networked, the security of the information systems utilized becomes even more essential and NTIA will work to ensure that it continues to manage risk to these essential systems.

The Administration views spectrum resources as a strategic asset for our economy and our national security. This means we must take a comprehensive, whole-of-government view on how to use spectrum and how to best unleash the power of spectrum-based technologies for the private sector. To accomplish this, we must follow several major principles.

The first of these is balance. We must balance the competing needs of all major equities to reach all of our national goals. For example, the Department of Defense is already devoting resources to adopt 5G technologies for national security and private sector satellite technologies that are interdependent with federal operations.

The second principle is to think long-term and comprehensively. We must develop an over-arching framework that will address new spectrum demands not just for today, but for the century to come.

The third principle is to be innovative and pioneering. This requires us to think beyond the traditional model of one allocation for one licensee for one use.

In October 2018, President Trump signed the "Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future." The memorandum set forth a "balanced, forward-looking, flexible, and sustainable approach to spectrum management" including the development of a new National Spectrum Strategy. To develop this Strategy, NTIA has worked with the Secretary's office, federal agencies, and the White House to detail a path for realizing the President's vision of a long-term spectrum infrastructure that sustains American technological dominance. As called for in the memorandum, federal agencies also identified their current spectrum usage and defined their anticipated future needs over the next 15 years.

Securing the Supply Chain

The telecommunications infrastructure is critical to nearly every aspect of the American economy and national security. The complex global telecommunications supply chain is increasingly vulnerable due to the proliferation of some foreign-sourced products and services. One way NTIA helps address these challenges is by supporting the Secretary of Commerce in implementing the President's Executive Order on Securing the Information and Communications Technology and Service Supply Chain.

NTIA also serves as a member of the executive committee of DHS's Information and Communications Technology (ICT) Supply Chain Risk Management Task Force, which provides advice and recommendations to DHS and private sector owners and operators of ICT critical infrastructure about how to assess and manage risks associated with the ICT supply

chain. Finally, NTIA strongly supports the recently updated version 1.1 of the NIST Cybersecurity Framework, which incorporates a new section helping organizations understand and manage supply chain risks.

The Department of Commerce is a member of the Federal Acquisition Security Council, which was established by the SECURE Technology Act. The council formalized aspects of several interagency efforts in which NTIA has participated, including the Supply Chain Risk Management Information Sharing Working Group led by the Director of National Intelligence; and the Section 889 Working Group, led by DHS and GSA. The Commerce representative to the Council brings economic impact analysis to bear related to the information and communications technology sector, identifies risks and unintended consequences of proposed actions, and explains communications sector incentive and market structures.

As a contributor to these efforts, NTIA has provided telecommunications subject matter expertise, as well as insight into cybersecurity vulnerability coordination and detection, the Internet of Things and next generation network security, and software component transparency, a critical component for minimizing, detecting, and mitigating supply chain risk.

FirstNet Resilience and Reliability

Congress created the First Responder Network Authority (FirstNet) in the Middle Class Tax Relief and Job Creation Act of 2012, Pub. L. No. 112-96, 126 Stat. 201 (2012), with the duty to ensure the deployment, operation, and maintenance of the nationwide public safety broadband network (FirstNet network), to address the lack of a standardized interoperable communications platform for first responders. The critical nature of first responders' communications demands that the network must be resilient and provide high availability, security, and privacy protections.

Cybersecurity is critical to the FirstNet mission to ensure all components of the FirstNet network are secure, reliable, and work together to provide first responders the data and communications they need on time, intact, and secure. From its inception, the FirstNet network has incorporated end-to-end cybersecurity for the network and its users. In partnering with AT&T, FirstNet invested years of planning and experience to create a secure environment for first responders. Among the key components of the enhanced cybersecurity of the FirstNet network design is the nationwide dedicated core network implemented by AT&T.

FirstNet network subscriber traffic running through the dedicated core ensures higher levels of reliability, redundancy, and protection through the dedicated processing and routing of the public safety traffic. Another critical enhancement can be found in the dedicated Security Operations Center (SOC), which handles continuous monitoring, detection, and mitigation efforts in cybersecurity for the network. The SOC provides 24/7/365 coverage and support for all cybersecurity considerations and is backed up by the full global network visibility of AT&T to ensure proactive protection for public safety.

From a cross-functional perspective, all aspects of cybersecurity are evaluated and reviewed within the context of the FirstNet network. This includes user equipment, such as phones, tablets, and in-vehicle routers, and anything that is connected to the network (i.e., the Internet of Things (IoT)). Similarly, there are processes in place for the vetting and inclusion of software applications developed for the public safety market.

Government and Industry Collaboration

To manage and address the risks posed by 5G, the U.S. government is taking an interagency approach to this issue, led by the Director of the National Economic Council (NEC) at the White House. The National Security Council (NSC) Cybersecurity Directorate and the NEC co-lead a regular 5G interagency Policy Coordination Committee through the National Security Presidential Memorandum - 4 process. These meetings are an opportunity to discuss and come to decisions on key 5G issues, such as work underway in standards bodies, as well as to provide updates on interagency 5G activities.

NTIA collaborates across the U.S. government and industry on numerous additional efforts related to the security of the nation's Internet architecture. We also have been working closely with the NSC staff and our interagency colleagues on implementing the National Cyber Strategy, which just marked its one-year anniversary. In that effort, we shared our activities across the interagency and looked for synergies to maximize the impact of the strategy. NTIA will continue to participate in these efforts.

3rd Generation Partnership Project

NTIA is a regular participant in the 3rd Generation Partnership Project (3GPP), which unites seven telecommunications standards development organizations from across the world and provides their members with a stable environment to produce the reports and specifications that define the 3GPP technologies behind today's ubiquitous mobile wireless networks and the emergence of 5G. 3GPP addresses cellular technologies, including radio access, security, core network and service capabilities that provide a complete system description for mobile telecommunications.

Cybersecurity Multistakeholder Processes

NTIA's cybersecurity multistakeholder processes contribute to the security of the nation's Internet architecture. Our ultimate objective is to foster a more resilient ecosystem through the creation of industry-led, market-based cybersecurity solutions. We think this kind of work can form the foundation of broader security baselines.

Most recently, NTIA has been working on software component transparency. Most modern software is not written completely from scratch, but includes existing components, modules, and libraries from the open source and commercial software world, which can be challenging to track. The IoT compounds this phenomenon, as new organizations, enterprises and innovators take on the role of software developer to add "smart" features or connectivity to their products. The sheer quantity of software inputs means that some products ship with vulnerable or out-of-date components.

NTIA convened a multistakeholder process late last year between software vendors and the enterprise customer communities who use these products. Stakeholders have talked to industry and government experts across the supply chain to capture their perspectives on how a software bill of materials, or "SBOM," is helping them today, and what they could do in the future if this practice became more widespread. We are working toward a shared vision of what the "minimum viable" implementation looks like, and how it can be implemented across the supply chain.

Botnet Coordination

Another example of NTIA's contribution to the protection of the Internet infrastructure is our work with NIST and DHS on the Botnet Report, and subsequent road map. Botnet attacks can have large and damaging effects, and they put the broader network at risk. The usual distributed denial of service (DDoS) mitigation techniques, including network providers building in excess capacity to absorb the effects, are designed to protect against botnets of a certain size. But much bigger botnets now capitalize on the sheer number of Internet of Things (IoT) devices.

The Botnet Report outlines a positive vision for the future, cemented by six principal themes and five complementary goals that would improve the resilience of the Internet ecosystem. For each goal, the report suggests supporting actions that can be taken by both government and the private sector. The Departments of Commerce and Homeland Security developed the report through an open and transparent process for the specific purpose of identifying stakeholder actions as opposed to government regulations. One of the report's focus areas was edge devices, including the components that go into them. Modern development techniques rely on a combination of open source and commercially available components. To meet future security demands, such components must be traceable through the supply chain and offer greater assurance.

Remediating botnet threats is an ecosystem-wide challenge that will take time to accomplish – we recognize that botnets are not going to be "solved" in one year. At the end of this year, the Departments of Commerce and Homeland Security will provide a status update to the President that reviews progress, tracks the impact of the road map and sets further priorities.

Conclusion

Deploying robust and secure 5G networks across the country will enable life-changing and life-saving advances from smart communities to the Internet of Things as well as technologies that will help to save lives and enhance our national security. The U.S. wireless industry has invested billions of dollars toward the development and deployment of new, powerful 5G networks.

However, the United States will only be able to harness the true economic and national security benefits of these networks if they are secure. NTIA is committed to coordinating across the Federal Government and engaging with the private sector to ensure this is the case. Thus, NTIA—and the Department of Commerce more broadly—are taking powerful steps to advance this technology to ensure the security of these networks and that the United States leads the world in 5G. We are focused on policies that will increase the amount of spectrum available for 5G, secure the supply chain, remove roadblocks to spur even greater investment in 5G, help make networks more secure and resilient against cyberattacks. Additionally, we support U.S. industry in global standards development as well as conduct and coordinate targeted research activities.

Thank you for the opportunity to participate in this hearing. I look forward to your questions.