TESTIMONY OF DIANE RINALDO

ASSISTANT SECRETARY FOR COMMUNICATIONS AND INFORMATION (ACTING)

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION (NTIA)

U.S. DEPARTMENT OF COMMERCE

HOUSE ARMED SERVICES SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES AND HOUSE OVERSIGHT AND REFORM SUBCOMMITTEE ON NATIONAL SECURITY

U.S. HOUSE OF REPRESENTATIVES

SEPTEMBER 10, 2019

Chairman Langevin, Chairman Lynch, and Members of the Committee:

Thank you for this opportunity to testify today on the role of the U.S. government in securing the nation's Internet architecture.

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 actors are seeking to influence the Internet's future, 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, encompassing exchange points, data centers, content delivery networks, the domain name system, undersea cables, and cable landing stations, as well as the diverse array of communications access networks and technologies that enable American consumers, businesses, and other institutions to connect to the Internet.

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 supporting the Secretary of Commerce as needed on the implementation of the Executive Order on Securing the Information and Communications Technology and Services Supply Chain.

NTIA is also the Executive Branch expert agency on issues relating to the Domain Name System (DNS), a critical component of the Internet infrastructure. The DNS functions similar to an "address book" for the Internet by allowing users to identify websites, mail servers, and other Internet destinations using easy-to-understand names (e.g., www.ntia.gov) rather than the numeric network addresses (e.g., 198.51.11.177) to look up information on the Internet. NTIA supports a multistakeholder approach to the coordination of the DNS to ensure the long-term viability of the Internet as a force for innovation and economic growth.

5G Security

The United States is dependent on reliable access to the finite resources that is radiofrequency spectrum. As with any critical resource, access to spectrum must be managed efficiently and effectively in order to achieve key economic and national security goals of the United States including the deployment of 5G networks and that our federal spectrum users, such as the Federal Aviation Administration (FAA), can operate its radio operations free from receiving harmful interference. 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.

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.

The Domain Name System

NTIA leads a longstanding interagency working group dedicated to matters pertaining to the Domain Name System (DNS). This DNS interagency working group includes representatives from the Department of Justice, Federal Bureau of Investigations, Department of Defense, Food and Drug Administration, Department of State, Department of Homeland Security (DHS), Internal Revenue Service, Department of the Treasury, U.S. Postal Service, U.S. Patent and Trademark Office, Secret Service, Security and Exchange Commission, the National Institute of Standards and Technology (NIST), and others. Through this interagency group, NTIA informs and coordinates with relevant agencies on matters pertaining to the security, stability, and resiliency of the DNS.

NTIA also oversees the management of the .us and .edu domains. In this role, NTIA coordinates responses to DNS incidents that pertain to these domains. Specific to .us, there are requirements associated with securing the name space and making it a safe and reliable domain. Under NTIA's oversight, both .us and .edu have implemented DNSSEC and employed other security and stability measures, and modernized their operations in a manner that improves the overall security of their domain space.

NTIA has a well-established relationship with the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a not-for-profit, public-benefit organization that oversees the operation of the Internet's DNS, coordinates allocation and assignment of the Internet's unique identifiers, such as Internet Protocol addresses, accredits generic top-level domain name registrars, and helps facilitate the voices of stakeholders worldwide who are dedicated to keeping the Internet secure, stable and interoperable.

NTIA was a leader in the creation of ICANN that evolved over the years through a series of legal agreements and contracts, and engages with ICANN and the broader global community on matters that are specific to ensuring the continued security, stability, and resiliency of the

DNS. Per statute, NTIA represents the U.S. Government in ICANN's Governmental Advisory Committee (GAC), which advises ICANN on public policy issues related to the Internet DNS. NTIA coordinates with other governments and stakeholders on domain name related security matters. For example, NTIA engaged the DNS interagency working group as well as Federal Chief Information Officers in preparation for the first-ever changing (rolling) of the DNS Security (DNSSEC) cryptographic key at the authoritative DNS root that took place in October 2018. NTIA will continue to work with agencies as well as other domestic and international partners in promoting DNSSEC implementation. Overall, NTIA's relationship with ICANN has proven useful in information exchange and coordinated response on all matters related to the DNS, including DNS based cyber incidents, DNS abuse, and strengthening the overall security of the DNS.

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.

FirstNet

Congress created the First Responder Network Authority (FirstNet) in the Middle Class Job Creation and Tax Relief Act of 2012 (P.L. 112-96) 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, such as 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.

Interagency Collaboration

NTIA collaborates across the U.S. Government on numerous efforts related to the security of the nation's Internet architecture. We have been working closely with the National Security Council (NSC) 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.

NTIA is engaged in numerous interagency efforts aimed at securing and increasing the resiliency of satellite systems, including representing executive branch equities on the encryption of telemetry, tracking, and command (TT&C) links and the development of policy guidance to help the owners and operators of critical infrastructure in their use of Global Positioning Systems (GPS) services.

Botnet Coordination

One significant example of NTIA's contribution to the protection of the Internet infrastructure is our work with NIST and DHS on the Botnet Report, delivered to the President in May 2018 in response to Executive Order 13800. 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. We have seen attacks that have topped a terabit per second. Dealing with a DDoS attack of this magnitude can take time, which is a major concern when mission-critical services are involved. Risks will increase as connected devices continue to proliferate.

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.

We are tracking progress through a document known as the Botnet Road Map. More than half of the identified tasks are already in progress or completed. Some of our private sector partners have already moved forward with supportive initiatives. For example, the Council to Secure the Digital Economy published its first International Anti-Botnet Guide late last year.

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.

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.

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. Several health care participants have demonstrated the value of SBOM through a proof of concept, by sharing data between a handful of large medical device manufacturers (Siemens, GE, Philips) and hospitals (Mayo Clinic, NY Presbyterian, Cedars-Sinai).

Conclusion

Over the past three decades, the Internet has been transformational for the American economy. According to the Bureau of Economic Analysis, the digital economy represented nearly 6.5 percent of the nation's GDP, or $1.2 trillion in 2016. America's established leadership in technology has resulted in millions of jobs and remarkable prosperity, and it also means that Americans rely on the Internet in their daily lives more than ever. Because of this, we must work harder than ever to ensure that the infrastructure supporting the Internet is secure.

NTIA is committed to coordinating across the Federal Government and engaging with the private sector to create a more secure Internet infrastructure. Security is the first step to ensuring that the United States can continue to harness the economic benefits of this vital part of the economy for American businesses and American workers as new technologies, including 5G, become integrated into our daily lives.

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