Written Testimony of Robert Mayer

Senior Vice-President Cybersecurity, USTelecom – The Broadband Association

before the House of Representatives Committee on Homeland Security

Public-Private Initiatives to Secure the Supply Chain

October 16, 2019

Chairman Thompson, Ranking Member Rogers, and other distinguished Members of the Committee, thank you for the opportunity to testify at today's hearing on Public-Private Initiatives to Secure the Supply Chain. My name is Robert Mayer and I am the Senior Vice-President Cybersecurity at USTelecom, the nation's trade association representing broadband providers, suppliers, and innovators connecting our families, communities and enterprises to the future. Our diverse membership ranges from large publicly traded global communications providers, manufacturers, and technology enterprises, to small companies and cooperatives – all providing advanced communications services to markets, both urban and rural and everything in between.

I also serve as the Chair of the Communications Sector Coordinating Council. I currently serve as co-Chair of the Department of Homeland Security Information and Communications Technology (ICT) Supply Chain Risk Management Task Force which is the subject of today's hearing.

The term supply chain management only entered the business lexicon in 1983 – when distributed computing power and new software applications were replacing traditional analogue forms of communications and record keeping. A decade later, the invention of the internet and the proliferation of e-commerce changed forever the pace, complexity and scale of commerce creating a global digital economy that now represents one fifth of the world's total economic value.

Today we stand at the precipice of an entirely new paradigm where technological advances in distributed computing, networking, fifth generation wireless, big data, artificial intelligence and machine learning promise to fundamentally change the nature of business transactions and the supply chain that is its foundation. The question we must now ask ourselves. What risks come with these transformational technologies and how best can we work together to mitigate them?

It's hard to overstate the complexity of supply chain challenges. For both suppliers and buyers, the potential universe of supply chain vulnerabilities touches all aspects of information technology— hardware and sub-components, IoT devices, operating systems, software and applications of all varieties, cloud and hosting services, telecommunications equipment or services. Essentially, any physical or logical element that can be used to generate, store, manipulate, or transport data in digital form. That means the billions of new connected objects coming online will expand the risk universe exponentially.

To be clear, many companies in the ICT ecosystem are incorporating high standards of supply chain risk management practices. Companies with large global and national footprints and substantial dependencies on foreign inputs, have dedicated teams of supply chain practitioners working tirelessly to ensure their brand is not tarnished and that their customers can continue to trust the integrity of their products and services. Rigorous internal systems and controls are applied and expectations of downstream suppliers are often reinforced by verified attestations, audits and contractual commitments.

The Task Force has addressed a small, but very important slice of the supply chain risk management universe. Working group 1, the information sharing group, has identified one of the most serious obstacles to effective risk management. Information about suspect suppliers cannot be freely exchanged when enterprises are subject to a variety of legal actions, including violations of federal or state anti-trust laws, anti-completive behaviors or deceptive trade practices. The working group has recommended that independent legal counsel study the matter more deeply with possible legislative or regulatory recommendations to reduce liability risk.

Working group 2 focused on the identification of processes and criteria to better understand and evaluate threats to ICT suppliers. That working group identified nine major threat categories comprising approximately 200 unique threats. The working group currently is framing work that might include examples of how enterprises can leverage the Task Force threat assessment as an information feed into their own company-specific risk management program.

Working Group 3 examined how Qualified Bidder and Manufacturer lists might help mitigate supply chain risk. The group examined five programs within the federal government that make use of such lists and identified several potential follow-up activities that would advance current and future use of such qualified lists.

Finally, Working Group 4 explored concerns related to deployment of counterfeit ICT products and recommended adding a new section to the Federal Acquisition Regulation (FAR). The section would be titled "Procurement of Information and Communications Technology from a trusted Original Manufacturer, the Authorized Channels or other Approved Source." That recommendation has been submitted to the Federal Acquisition Security Council for Review.

The Task Force's importance and value is not only reflected in the sum of its current and future work but also because it is a model for collectively advancing policies critical to our national interests that can be operationalized in ways that have a high likelihood of success. The Task Force's success did not happen overnight; it is the result of more than a decade of an increasingly robust, mutually accountable and trusted public-private partnership. The Task Force's governance structure supports the important principle of a whole-of government approach and has brought an extraordinary group of private and public sector experts to the same table to tackle some of the most challenging supply chain issues. I know I speak for all of the members of the Task Force when I say we appreciate the gravity and urgency of our work, and we are committed to delivering strategies that will lead to meaningful and sustainable solutions.

Thank you for the privilege of participating in this hearing. I look forward to answering your questions.