ITI Promoting Innovation Worldwide

Written Testimony of

John S. Miller
Vice President of Policy and Senior Counsel
Information Technology Industry Council (ITI)

Before the

Committee on Homeland Security

U.S. House of Representatives

Public-Private Initiatives to Secure the Supply Chain

October 16, 2019

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Written Testimony of
John S. Miller
Vice President of Policy and Senior Counsel
Information Technology Industry Council (ITI)

Before the
Committee on Homeland Security
U.S. House of Representatives

Public-Private Initiatives to Secure the Supply Chain

October 16, 2019

Chairman Thompson, Ranking Member Rogers, and Distinguished Members of the Committee on Homeland Security, thank you for the opportunity to testify today. I am John Miller, Vice President of Policy and Senior Counsel at the Information Technology Industry Council (ITI).[1] I have deep experience working on public-private security initiatives in the United States, including serving as the current Chair of the Information Technology Sector Coordinating Council (ITSCC)[2] and Co-chair of the Information and Communications Technology Supply Chain Risk Management Task Force (Task Force). I am honored to testify before your Committee today on the important topic of *Public-Private Initiatives to Secure the Supply Chain*. The global ICT industry respects and takes seriously the U.S. government's – and other governments' – obligation to address risks to global information and communications technology (ICT) supply chains, and the responsibility of governments to protect national security more broadly. We believe government and industry must work together to achieve the trusted, secure, and reliable global supply chain that is a necessary priority for protecting national security and is also an indispensable building block for supporting innovation and economic growth. We welcome the Committee's interest and engagement on this subject.

ITI represents nearly 70[3] of the world's leading ICT companies. Robust security is a key pillar of building and maintaining trust in the global ICT ecosystem, and is thus essential to our businesses and customers. Supply chain security and cybersecurity are rightly priority issues for governments and our industry, and we share the common goals of improving

[1] The Information Technology Industry Council (ITI) is the premier advocacy and policy organization for the world's leading innovation companies. ITI navigates the constantly changing relationships between policymakers, companies, and non-governmental organizations to promote creative policy solutions that advance the development and deployment of technology and the spread of digitization around the world. Visit https://www.itic.org/ to learn more.

[2] The Information Technology Sector Coordinating Council (IT SCC) serves as the principal entity for coordinating with the government on a wide range of critical infrastructure protection and cybersecurity activities and issues. The IT SCC brings together companies, associations, and other key IT sector participants, to work collaboratively with the Department of Homeland Security, government agencies, and other industry partners. Through this collaboration, the IT SCC works to facilitate a secure, resilient, and protected global information infrastructure. Visit https://www.it-scc.org to learn more.

[3] See ITI membership list at https://www.itic.org/about/membership/iti-members.

cybersecurity and supply chain security, protecting the privacy of individuals' data, and maintaining strong intellectual property protections. Further, our members are global companies and do business in countries around the world. Most service the global market via complex supply chains in which products are developed, made, and assembled in multiple countries, and service customers across all levels of government and the full range of global industry sectors, such as financial services, healthcare, and energy. We thus acutely understand the importance of securing global ICT supply chains as not only a global business imperative for companies and customers alike, but as critical to our collective security. As a result, our industry has devoted significant resources, including expertise, initiative, and investment in cybersecurity and supply chain risk management efforts to create a more secure and resilient Internet ecosystem.

Our members also understand we cannot tackle current and future cybersecurity challenges on our own. We recognize public-private partnerships and other multi-stakeholder approaches are essential to addressing our shared security challenges and have thus prioritized working with governments around the world to help develop cybersecurity and supply chain security policy solutions. We believe the emergence of supply chain security as a priority issue amongst government policymakers globally highlights the urgency with which like-minded nations must address this issue. It also represents an important opportunity for U.S. policymakers to advance supply chain security policy approaches that are not only compatible with, but indeed drive, global policymaking in this space. Working together to leverage the public-private partnership structures that were pioneered in the United States, as well as sound risk-management based approaches that we have long advocated as best cybersecurity practices, industry and government can seize this moment to lead on supply chain security policy together.

I will focus my written testimony on four areas: (1) **the evolving supply chain threat** and the need for public-private action; (2) **the creation of the Task Force** grounded in principles of risk management and public-private partnerships; (3) **the progress of the Task Force to date**, including the recently released Interim Report and the Task Force's work to help the Department of Homeland Security (DHS) implement the supply chain Executive Order (EO); and (4) **recommendations on a collaborative path forward,** including discussing how the Federal Acquisition Security Council (the "FASC") and other federal government stakeholders can synergistically work with the Task Force to help advance our collective supply chain security policy interests.

1. The Evolving Supply Chain Threat

While supply chain security is not a new topic, particularly for large technology companies managing sophisticated global supply chains, the heightened policymaker focus on the issue over the past two years is unprecedented. The increased focus on supply chain security, by governments, policymakers and private sector actors, is prompted by a few key developments.

A Multifaceted and Growing Threat. Supply chain risk management (SCRM) has always been a multifaceted challenge. On the one hand, SCRM is one element of an organization's overall cybersecurity risk management program (indeed, the visionary Cybersecurity

Framework developed in the U.S. integrated SCRM into Version 1.1 in 2018). On the other hand, a SCRM program must address much more than just cybersecurity threats to IP, systems and networks, but also threats that are physical (e.g. building security), personnel-based (e.g. insider threats), economic (e.g. cost-volatility), legal (e.g. weak IP laws), development or manufacturing related (e.g. compromises in system, hardware, or software development lifecycle processes or tools), or external threats such as those related to environmental, geopolitical or workforce related factors.

When we consider our increasingly connected global ICT digital infrastructure and economy, and acknowledge the reality that ICT products, hardware, software, and services are powering every segment of the economy as we move toward surpassing 20 billion connected devices in 2020,[4] one can better appreciate the vast scope of risks to the global ICT supply chain "attack surface" that we need to secure. Nation state threats, too, are a greater part of the conversation than before, implicating not only national security but also economic security and U.S. competitiveness.

Putting both of those pieces together – the large and growing number of all-hazards threats and the vast and increasing number of products and services generated by the global ICT supply chain – we can better appreciate the scope of the risks that must be managed, and the scope of the policy challenge.

The Rise of 5G and Data. The buildout of 5G networks has magnified the spotlight on supply chain security challenges, where the focus has largely been on anticipated risks. While securing the 5G infrastructure, including both networks and component ICT parts, is of course critical, it bears noting that 5G networks and equipment will also contain security enhancements that can help make 5G networks more secure than previous generations. Rather, it is the increased speed and volume of data that will soon flow through 5G networks, helping to enable the next generation of data-enabled innovations such as the internet of things (IoT) and artificial intelligence (AI), that has driven the United States and other governments to more intensely focus on global supply chain security threats.

As the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) documents in its 5G Risk Assessment,[5] 5G networks will enable increased speeds and amounts of data that are staggering. The data flowing through 5G networks, or throughput, will be multiplied by a factor of up to 200. The speed at which data travels, or latency, will be up to 20 times faster than in 4G networks. The implications of these numbers are significant – not only because 5G will power the next wave of data-driven innovations such as IoT and AI, but also because the question of who potentially has access to or controls that data raises a panoply of questions, including implications for individual privacy, national security, technological leadership, and economic competitiveness. The

[4] "Leading the IoT, Gartner Insights on How to Lead in a Connected World", Mark Hung, 2017, available at: https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

[5] " Overview of Risks Introduced by 5G Adoption in the United States", Cybersecurity and Infrastructure Security Agency (CISA), July 31, 2019, available at: https://www.dhs.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf

centrality of data to our present and future lives and to the supply chain debate underscores that SCRM must focus on managing potential vulnerabilities and other malicious activity targeted at ICT supply chains as well as the potential for governments or others perceived as adversaries to access that data through their domestic legal regimes.

While it will be important to continue to focus on ICT SCRM, and creating high assurance, trusted ICT products, we must realize that managing the full range of data access risks implicated by the current SCRM debate moves us into somewhat uncharted territory.

Increase in Supply Chain Policymaking. We appreciate the focus of governments and policymakers globally on the urgency of addressing supply chain risk, for all the reasons stated above. However, the sheer volume of policymaking activity has, in some instances, overwhelmed the ability of private sector entities, particularly small and medium-sized businesses (SMBs), to effectively monitor, make sense of, and implement important supply chain policy or legal developments. While well-intended, some policies may have unintended consequences on security, innovation, and competitiveness – which is why public-private sector cooperation is imperative. To ensure these measures can be properly addressed and implemented, is critical that this activity is coordinated and targeted at identified legal or policy gaps.

Global government activity regarding supply chain security is rising across the EU, and in countries including Japan, Australia and elsewhere. In the U.S. there continues to be significant and not always visible activity across multiple federal agencies, and the last few years have brought multiple legislative efforts from Congress, including numerous stand-alone bills and National Defense Authorization Act (NDAA) amendments, as well as President Trump's recent supply chain EO, and the launch of the FASC following last year's *SECURE Technology Act*. The Task Force helps drive a more holistic, coordinated approach through a better understanding of supply chain policymaking activity in the United States and holds the promise to help streamline efforts to address potential risks.

2. The Creation of the Task Force Grounded in on Principles of Risk Management and Public-Private Partnerships

While formation of the Supply Chain Task Force was motivated out of a heightened concern regarding supply chain threats, its formation, structure and mandate are grounded in cyber and supply chain security principles long advocated by the ICT industry. Those principles are based on the importance of taking risk-management based approaches to complex threats such as global ICT supply chain security threats and the promise of public and private stakeholders working together through partnerships to forge durable solutions to those threats.

Approaches to Risk Management: No One Size Fits All. The ICT industry has long maintained that efforts to improve cybersecurity, including supply chain security, must be based on effective risk management of a dynamic and ever-evolving set of threats.

Cybersecurity is not an end state, but rather a continuous process of protecting the global digital infrastructure and its users. No sector of the economy is without some inherent risk, whether that is the result of a natural disaster, a malicious automated attack, or simple

human error. As cyber and supply chain attacks become increasingly more sophisticated, the adoption of comprehensive risk management strategies is critical for organizations of all sizes and across all sectors, particularly those managing complex global supply chains. By integrating technologies, people, and processes into an overall risk management framework, limited resources can be most efficiently focused on where the need is greatest.

Effective risk management allows individuals and entities to properly identify, assess, prioritize, and manage threats to their data, systems, and operations, including supply chains. There is no one-size-fits all approach. Eliminating one potential threat may unintentionally create other vulnerabilities. For example, using the same supplier (even a "trusted" supplier) throughout a network or supply chain could make it easier to exploit a vulnerability; thus, a diversity of suppliers is crucial to risk management. The National Institute of Standards and Technology (NIST) Cybersecurity Framework, informed by a collaborative effort involving public and private sector stakeholders, provides a familiar example of a flexible risk management tool that can help a diversity of entities – critical infrastructure owners and operators, government agencies, and other stakeholders – understand how to approach cybersecurity risk management. Notably, Version 1.1 of the Framework, published in 2018, incorporates SCRM standards, guidelines and best practices.

Global ICT companies build risk management into their daily operations and long-term planning, including efforts to secure their supply chains, through mechanisms like legal and contractual agreements, cybersecurity operational controls, adherence to global risk management standards, and a host of other practices. As the primary owners and operators of critical cyber infrastructure, the private sector has devoted significant resources, including expertise, initiative, and investment in cybersecurity and risk management efforts to create a more secure and resilient Internet ecosystem. However, the ICT industry understands it cannot tackle current and future cybersecurity challenges on its own.

Public-Private Partnerships Are Essential. Public-private partnerships and other multi-stakeholder approaches are essential to addressing supply chain security. Government and industry often have access to unique information sets – only when this information is shared can all relevant stakeholders see the complete picture. These partnerships are essential to 1) identify potential threats; 2) understand how and whether the risk can be managed; and 3) determine what actions should be taken to address risks without yielding unintended consequences. The private sector ICT community has been foundational in developing the infrastructure of cyberspace and, for well over a decade, has provided leadership, innovation, and stewardship in all aspects of cybersecurity, including helping to develop and participating in numerous public-private partnership structures and efforts.

Sector Coordinating Councils. Global ICT companies participate in sector coordinating councils (SCCs), which are self-organized, self-governed councils that allow owners and operators of critical infrastructure to engage on a range of sector-specific strategies, policies, and activities. SCCs also enable participants to coordinate with their sector-specific

agencies and related Government Coordinating Councils (GCCs) to facilitate government collaboration on a range of critical infrastructure security policy and strategy issues, including on supply chain security. I am pleased to chair the ITSCC and to work closely with my counterparts in the Communications SCC, as well as DHS as our sector-specific agency and other U.S. government partners, on the Task Force.

Formation of the Task Force. The Task Force embodies these critical dual principles of risk management and public-private partnership. The Task Force aims to better secure global ICT supply chains, gathering stakeholders from key communities – including from the communications and IT sectors, as well as across multiple federal agencies, including Departments of Homeland Security, Commerce, Defense, Treasury, Justice, and Energy; Office of the Director of National Intelligence (ODNI), National Security Agency (NSA), General Services Administration (GSA), Social Security Administration (SSA), National Telecommunications and Information Administration (NTIA), Federal Communications Commission (FCC), NIST, NASA, and others. These entities should work together to enable targeted resource investment, share technical and policy expertise, and identify actionable policy solutions aimed at helping public and private stakeholders better manage ICT supply chain risks.

From the perspective of the IT sector – both ITI and the ITSCC – there was no hesitation regarding the merits of Task Force participation. Supply chain security had been identified as the top cybersecurity priority of both organizations, and many experts across the sector who had been working on this issue for a long time shared the view that this was a moment in time where real progress could be made.

There was also widespread agreement that the challenges quite clearly are shared by government and the private sector – and thus adequately addressing them requires a collaborative, holistic approach involving the IT and Communications sectors working together with U.S. government partners from key federal agencies.

3. Progress of the Task Force to Date

The Task Force was chartered in late 2018 by DHS and CISA working with the IT and Communications SCCs, with the express purpose of providing guidance and recommendations to government and private sector critical infrastructure owners and operators to help them better assess and manage risks associated with the global ICT supply chain.

Comprised of 60 voting members -- 20 IT companies and associations, 20 communications sector stakeholders, and 20 representatives from across the U.S. government -- the Task Force acts as a forum for private sector and government collaboration on methods and practices to effectively identify, prioritize, and mitigate ICT supply chain risks, with the goal of providing realistic, actionable, timely, economically feasible, scalable, and risk-based recommendations for addressing those risks. Beyond its voting membership, scores of other entities have additionally participated in the Task Force at the working level.

Once we were up and running, the Task Force members surveyed the vast supply chain threat and risk management landscape, identifying four initial working groups focused on

both longer term, foundational efforts that could have global ICT ecosystem-wide impact and shorter-term tactical efforts geared toward shoring up the federal government's supply chain: (1) development of a common framework for the bi-directional sharing of supply chain risk information between government and industry; (2) identification of processes and criteria for threat-based evaluation of ICT supplies, products, and services; (3) identification of market segments and evaluation criteria for Qualified Bidder and Qualified Manufacturer lists to address considerations of vendor and product inclusion and exclusion; and (4) policy recommendations to incentivize purchase of ICT from original equipment manufacturers (OEM) and authorized resellers.

Interim Report. The Interim Report,[6] published in September 2019 at CISA's 2nd Annual Cybersecurity Summit, provides a fuller summary of the Task Force's origins, membership, and workstreams, and also details progress to date on each of those workstreams. Rather than restating all that information in my testimony, I thought the Committee would find it more helpful if I highlighted a few key takeaways:

Information sharing remains a key priority. Working Group One made excellent progress exploring the types of information that would be most valuable in mitigating supply chain risk; whether that information exists in a standardized or easily accessible form or from sources that can be easily identified, accessed and leveraged for risk management purposes; and what barriers might exist that are impeding the collection and or dissemination of such information. While Working Group One determined that many types of risk information are indeed available, the sources were not always easily known and did not typically exist in a standardized format (unlike cyber threat indicators in the cybersecurity threat information sharing context). Additionally, due to the wide array of supply chain threats, such information was not easily centralized nor accessible.

Working Group One significantly determined that the highest value supply chain threat information relates to suspected, known, or proven bad actors in the supplier context, but that legal and policy issues often prevent the sharing of such information. The Working Group concluded that further legal analysis and guidance are thus prerequisite to fully developing the envisioned bi-directional supply chain information sharing framework. This foundational work will likely be carried forward into year two of the Task Force and may well presage the need for future legislative action to remove legal barriers to effective sharing of SCRM threats.

The supply chain threat landscape is vast. The efforts of Working Group Two help illustrate the vast threat space in play when we consider scope of global ICT supply chain challenges. Working Group Two was established to identify processes and criteria for threat-based evaluation of ICT suppliers, products, and services. The working group concentrated on threat evaluation related to suppliers as an initial matter, rather than risk assessment, to ensure it was looking more broadly at the breadth of the SCRM ecosystem, rather than at

[6] "Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report: Status Update on Activities and Objectives of the Task Force," CISA, September 2019, available at: https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf

risks associated with specific ICT products and services.[7] The working group methodically identified and inventoried the global supply chain threat landscape, compiling nearly 200 supplier-related threats and categorizing those threats into nine categories to provide a helpful taxonomy. The threat categories included counterfeit parts, cybersecurity, internal security operations and controls, compromise of system development lifecycle and tools, insider threats, inherited risks (extended supply chain), economic, legal, and external end-to-end threats ranging from natural disasters to workforce and labor issues.

The Working Group then developed several threat scenarios, ranging from ransomware attacks to natural disasters, and reviewed and documented those scenarios to provide additional context regarding the threat, its importance and potential impact on the supply chain, as well as information related to threat sources, vulnerabilities, and potential mitigations. Next steps for the Working Group could include creating a similar inventory and taxonomy of threats related to ICT products and services (as per the group's mandate) and providing a similar assessment of various threat scenarios related to those products. In any event, the foundational work around threat evaluation has already informed the work of other Task Force working groups, and as the work product matures can prove invaluable for informing future government and private sector SCRM activities.

We need to continue to explore the extent to which we can leverage public sector SCRM solutions in the private sector and vice versa. Working Groups 3 and 4 tackled tactical issues more immediately relevant to federal government SCRM and procurement, including identification of market segments and evaluation criteria for Qualified Bidder (QBL) and Manufacturer (QML) lists (Working Group 3) and policy recommendations to incentivize the purchase of ICT from OEMs, authorized channels, or other trusted suppliers (Working Group 4). Whether and how to use QBLs and QMLs is a topic with different implications in the public procurement and private sector contexts. For instance, many global companies currently manage trusted supplier programs and there are lessons that could be leveraged in federal procurement. However, the process of qualifying suppliers in the public sector procurement context could have a disproportionate impact on SMBs if not managed carefully. These are the types of issues Working Group 3 will continue to explore. In the case of Working Group 4, the primary tasking of the group was completed with the delivery of its policy recommendation, *Procurement of ICT from OEMs, their Authorized Channels, or other Trusted Suppliers*, and is primarily geared toward addressing risks associated with the procurement of potentially counterfeit products from the gray market or other unauthorized channels. The efforts of Working Group 4 illustrate the Task Force's capability to rapidly conclude targeted projects and make recommendations that can translate into policy solutions in the short term.

Urgent Supply Chain Inventory Work. As the Interim Report indicates, good progress was made on compiling a private sector inventory of SCRM standards, guidance, and best

[7] Working Group 2 determined that "risk" is the intersection of assets, threats, and vulnerabilities. A vulnerability is a shortcoming or hole in the "security" of an asset. Risk represents the potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

practices. This inventory work product will provide invaluable guidance that companies and federal government agencies can use to better inform their supply chain risk management activities. A parallel effort to compile supply chain risk management efforts across the federal government is still in flight. When completed and shared, the government inventory will assist the Task Force members as they consider future workstreams and can serve as a resource for policymakers in Congress and elsewhere as they consider which aspects of the multifaceted supply chain issue to address via legislation. Further, the government inventory will bring clarity to the supply chain risk management landscape for those stakeholders who have expressed concern that that the volume of supply chain risk management activity is difficult to effectively monitor.

Collaboration with FASC. The Task Force is also coordinating efforts with the Federal Acquisition Supply Chain (FASC) to help ensure the effectiveness of the implementation of the *Federal Acquisition Supply Chain Security Act (FASCSA)* (passed late last year as part of the *SECURE Technology Act*). Having established the connective tissue between the Task Force and the FASC over the past several months, the Task Force is poised to help inform the interim implementing rules for FASCSA due at the end of 2019 and the final rules due in 2020, as well as to advance a number of other interagency supply chain risk management priorities.

Collaboration on the Supply Chain EO. In addition to its regular workstreams, the Task Force also stepped in to assist DHS as it fulfilled its duties pursuant to *Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain* (Supply Chain EO), which tasked DHS with producing a report assessing the criticality of ICT products and systems. Task Force members provided required private sector input to CISA's National Risk Management Center (NRMC), which was delegated the responsibility of conducting the ICT criticality assessment required by the Supply Chain EO. This input resulted in a deconstruction of the ICT supply chain into five roles, 11 sub-roles, and 61 elements (ICT hardware software and services). DHS has stated that it hopes this elemental deconstruction will provide a helpful and standardized taxonomy for discussing ICT criticality within the Task Force and elsewhere.

The initial assessment focused on ICT products and services comprising the "connect" theme of the National Critical Functions list (primarily covering the backbone of national connectivity enabling cross-country and global core telecommunications networks and services), and future assessments will address other themes identified by the NRMC in the National Critical Functions (NCFs)[8]. As we understand it, the assessment will inform the Commerce Department's promulgation of rules to implement the Supply Chain EO, and the assessment may help inform any future work taken on by the Task Force to assess threats associated with ICT products and services. The deployment of the Task Force to assist in producing the ICT assessment helps illustrate the value of the partnership as a durable resource to assist government policymakers implement SCRM policies.

[8] "National Critical Functions Set (NCFs)", CISA, April 2019, available at: https://www.dhs.gov/sites/default/files/publications/national-critical-functions-overview-508.pdf.

4. Recommendations on a Collaborative Path Forward

My testimony thus far illustrates the substantial amount of progress that has been made by the Task Force, but also recognizes that there is much work still to be done. While the Task Force intends to continue to advance the ball on multiple SCRM projects during year two of its mandate, below are concrete recommendations for U.S. government actions on how to maximize the impact and effectiveness of the Task Force's work to aid in other federal supply chain efforts, as well as recommendations for broader strategic U.S. government action to address global SCRM challenges.

Build Out the Established Connective Tissue between the Task Force and the FASC. Structurally, the established connective tissue between the Task Force and the FASC creates real opportunities for the FASC to leverage the private sector expertise assembled in the Task Force to help build out the rules to implement the FASCSA. Involving the Task Force in its efforts with more regularity can help the FASC achieve the bill's objectives for better securing the federal government's supply chain, while minimizing unintended impacts to continued technology innovation and the technological leadership of US companies.

Prioritize Communicating the Task Force Inventory Results to Key Stakeholders and Integrate the Inventory Results into SCRM Policy Planning. Soon after the Task Force's inception, we reached consensus that conducting an inventory of public sector supply chain activities would be useful to help bring order to the scores of disconnected ongoing SCRM efforts across the federal government. Taking a strategic approach, the Task Force's goal in recommending the government conduct such an inventory was that by taking stock of the various existing and ongoing supply chain efforts we could prevent duplicative efforts, and identify what work needed to be done. After completion and review of existing efforts (which will essentially provide a gap analysis), both the Task Force and other stakeholders will be better situated to: (1) identify what tasks aren't being done and prioritize those that are most important and needed; (2) identify tasks that are most well-suited to be completed by the Task Force; and (3) identify what tasks are important, but should be completed by others (such as by Congress in instances where changes to legal authorities are needed to implement SCRM improvements).

Embrace the Task Force as the center of gravity for public-private collaboration on SCRM. The Task Force could also help increase visibility of the ongoing efforts and construct a narrative to articulate how everything fits together. If we take this type of strategic 360-degree approach to the problem, we can essentially position the Task Force as the central hub for all the many ongoing and disconnected supply chain efforts across the U.S. government and industry more broadly. Other stakeholders, including Congress, will at least indirectly benefit from cementing the Task Force as an SCRM resource.

Further streamline USG supply chain efforts. To help mitigate current and ongoing SCRM risks, we recommend that Congress work with the administration in streamlining existing and new tools on supply chain issues (including the FASC, FASCSA implementation, and Supply Chain EO) to better align resources and avoid duplicating efforts and support long-

term, coordinated solutions to address global supply chain challenges. The government inventory can play a key role here.

Target Future Supply Chain Measures to Identified Gaps. The Task Force learned quickly through our initial scoping activities that attempting to "boil the ocean" to "solve" supply chain security challenges would be a fruitless task. Instead, we worked to target both foundational and tactical workstreams that could tackle discrete elements of the issue, while also laying the groundwork for future success. Laws, regulations, and other measures to address supply chain security risks should take a fact-based, narrowly tailored approach to combat concrete and identifiable risks, rather than apply broadly to entire categories of technology or business activity.

Deepen Engagement with International Partners and Pursue a Coordinated Approach. Global ICT SCRM challenges ultimately call for globally scalable solutions, and we encourage cross-border collaboration on this issue. The United States and other open economies should take common approaches to technology-related national security risks – including through promotion of global, consensus-based, industry-led standards – to avoid harmful fragmentation of markets. The *Prague Principles on 5G Security*[9] provide a good blueprint for this sort of activity.

Conclusion

Members of the Committee, ITI and our member companies are pleased you are examining how public-private partnerships play a key role in addressing evolving and increasingly sophisticated supply chain threats.

Historically, the United States has maintained a leadership position in cyberspace – from the companies who have led the way in building the global digital economy and internet-based services that have fueled its growth, to visionary cyber policy developments such as the Cybersecurity Framework, to pioneering the use of cybersecurity public-private partnerships. The U.S. government should aspire to maintain a similar leadership position going forward on SCRM policy, and to do so it must work collectively, via public-private collaboration and across sectors, both domestically and on the global stage.

ITI stands ready to provide you any additional input and assistance in our collaborative efforts to develop policy approaches to supply chain security that continue to leverage risk management-based solutions and public-private partnerships as the most promising way forward for addressing complex and evolving global ICT supply chain threats.

I thank the Chairman, Ranking Member, and Members of the Committee for inviting me to testify today and for their interest in and examination of this important issue. I look forward to your questions.

Thank you.

---

[9] "The Prague Proposals: The Chairman Statement on Cybersecurity of Communication Networks in a Globally Digitalized World." May 3, 2019, available at: https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf