Written Testimony of

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

Before the

Committee on Commerce, Science, and Transportation

United States Senate

Implementing Supply Chain Resiliency

July 15, 2021

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

Before the
Committee on Commerce, Science and Transportation
United States Senate

Implementing Supply Chain Resiliency

July 15, 2021

Chair Cantwell, Ranking Member Wicker, and Distinguished Members of the Committee on Commerce, Science and Transportation, thank you for the opportunity to testify today. I am John Miller, Senior Vice President of Policy and General Counsel at the Information Technology Industry Council (ITI).[1] I have deep experience working on public-private supply chain policy initiatives in the United States, including serving as the current Co-chair of the Cyber and Infrastructure Security Agency (CISA)-sponsored Information and Communications Technology Supply Chain Risk Management Task Force (ICT SCRM Task Force)[2] as well as Vice Chair of the of the Information Technology Sector Coordinating Council (ITSCC).[3] I am honored to testify before your Committee today on the important topic of *Implementing Supply Chain Resiliency*. The global information and communications technology (ICT) industry respects and takes seriously the U.S. government's (USG) obligation to address the resiliency of global supply chains, including the ICT supply chain. We believe the USG and industry must work together, along with partners and allies, to achieve the trusted, secure, reliable, and resilient global supply chains that are a necessary priority for protecting national security and are also an indispensable building block for supporting competitiveness, innovation, and economic growth. We welcome the Committee's interest and engagement on this subject.

[1] The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, manufacturing, and related industries. Visit https://www.itic.org/ to learn more.

[2] The ICT Supply Chain Risk Management (SCRM) Task Force—sponsored by CISA's National Risk Management Center (NRMC)—is the United States' preeminent public-private supply chain risk management partnership, established in response to these realities and entrusted with the critical mission of identifying and developing consensus strategies that enhance ICT supply chain security. The Information Technology Sector Coordinating Council and Communications Sector Coordinating Council are co-chartering entities of the Task Force along with NRMC. Visit https://www.cisa.gov/ict-scrm-task-force to learn more.

[3] 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, cybersecurity and supply chain risk management 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.

ITI represents 80 of the world's leading ICT companies.[4] Most of ITI's members service the global market via complex supply chains in which technology is 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. Thus we acutely understand the importance of ensuring the resiliency of global ICT supply chains as not only a global business imperative for companies and customers alike, but as critical to our collective national and economic security. As a result, our members have 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, inclusive of ICT supply chains.

Last month, ITI welcomed the Senate's passage of the *U.S. Innovation and Competition Act (USICA)* as critical to helping the United States remain competitive on the international stage by prioritizing and expanding essential investments in research, development, and technological advancement. USICA takes important steps to expand U.S. innovation leadership, including key measures to help build a strong ecosystem for developing advanced technologies and creating new jobs in communities across the country. ITI was particularly pleased that the bill provides robust funding for the *CHIPS for America Act (CHIPS)* to boost U.S. investments in the semiconductor ecosystem – including promoting a strong, skilled workforce for advanced manufacturing, strengthening the semiconductor supply chain, and increasing U.S. manufacturing capacity – all of which are essential for U.S. economic and national security.

We were similarly pleased to commend the White House's publication of the final report stemming from the 100-Day Reviews under Executive Order 14017 on *America's Supply Chains (ASC EO)* just a couple of days after *USICA's* passage, which signaled the Biden Administration's commitment to building trusted, secure, and resilient supply chains and echoed some of USICA's key proposals. Importantly, the administration outlined a clear vision to strengthen U.S. semiconductor leadership, including efforts to address research and development, increase manufacturing, and build a skilled workforce, a forward-looking and complementary approach to enhance economic competitiveness and bolster national security. Together, these mutually reinforcing steps taken by the administration and Congress hold the promise of making the U.S. – and ultimately global – supply chains stronger and more resilient, advancing U.S. competitiveness, and harnessing U.S. innovation.

Of course, acknowledging the pressing global supply chain resiliency challenges laid bare by the COVID-19 pandemic and crafting sound policies to address them does not necessarily guarantee the successful execution of those policies. So the key question – as the subject of this hearing foreshadows – is how can we most effectively implement recent Congressional and administration policies to improve supply chain resiliency?

I will focus my written testimony on four areas bearing on this question: (1) **the importance of a strategic, holistic and coordinated approach to addressing supply chain resiliency** including the need to prioritize public-private collaboration; (2) a discussion of **the Biden Administration's emerging approach to supply chain resiliency and the relevant provisions of USICA**; (3) **the U.S. Department of Commerce's (Commerce) increasingly important role in supply chain resiliency and security, and its recent track record of implementing supply chain policy initiatives**, including various taskings from the prior administration; and (4) **recommendations for how Commerce and**

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

the USG more broadly can most effectively implement supply chain resiliency going forward.

1. A Strategic, Holistic and Coordinated Approach is Foundational to Implementing Supply Chain Resiliency

While supply chain resiliency is not a new topic, particularly for large technology companies managing sophisticated global supply chains, the heightened U.S. policymaker focus on supply chain resiliency and security over the past few years is unprecedented, as evidenced by the more than 30 active federal supply chain security and resiliency measures inventoried by the ICT SCRM Task Force since late 2018. The palpable impacts of the COVID-19 pandemic on global supply chain resiliency further intensified the focus on this issue. The increased policy attention on supply chain issues prompted ITI earlier this year to prominently feature recommendations regarding supply chain security and resiliency in our *Policy Memo for the Biden-Harris Administration and 117th Congress*[5] and issue a set of *Supply Chain Security Principles*[6] intended to lay out strategic considerations to guide U.S. policymakers tackling these issues in 2021 and beyond.

Although supply chain security and resiliency are not one and the same, they are closely related insofar as national security (including cybersecurity), trustworthiness, availability and competitiveness are all facets of the broader term resiliency, and ITI's recommendations are applicable across both concepts.

Our recommendations noted the change in administrations and a new Congress offered the opportunity for a strategic review of U.S. supply chain security and resiliency policy to develop a more coherent, streamlined, and effective long-term approach, consistent with the holistic assessment of the ICT and other industrial base supply chains called for by the *ASC EO*.

Key pillars of ITI's recommendations in this regard have consistently included the following:

Pursuing a holistic, streamlined, coherent, and strategic approach to supply chain resiliency and security policy. The federal government's ability to provide consistent regulatory approaches and supply chain security guidelines is critical to securing the U.S. innovation economy and ensuring supply chain resiliency. ITI shares the concerns of members of this Committee regarding threats to global ICT supply chains, which implicate cybersecurity, national security, economic security, and U.S. competitiveness. However, these legitimate concerns have too often manifested in uncoordinated, inconsistent approaches across various departments and agencies. We have encouraged the establishment of a lead agency on supply chain risk management to manage a coordinated and effective approach to varied and disparate activities occurring at all levels of government.

Promoting a thoughtful, harmonized, risk-based, evidence-driven approach to supply chain resiliency policy to facilitate transparency and predictability. The approach to supply chain security over the last several years has primarily focused on country-of-origin, particularly China, which has led to an over-reliance on this attribute and short-circuited more fulsome risk analysis. While country-of-origin is one risk factor bearing on supply chain security as well as resiliency, it

[5] See ITI's *Policy Memo for the Biden-Harris Administration and 117th Congress: Advancing Innovation to Make the U.S. More Globally Competitive* at https://www.itic.org/documents/general/ITI_CompetitivenessMemo_Final.pdf.

[6] See ITI's *Supply Chain Security: Principles for Strategic Review* at https://www.itic.org/policy/ITI_SupplyChain_Principles2021.pdf.

should not be the sole and dispositive factor animating U.S. supply chain policy, or in determining trustworthiness. It is noteworthy that the ICT SCRM Task Force working group on Threat Assessment catalogued a total of 188 supplier-related threats, with country of origin being just one. A successful supply chain resiliency strategy must widen the aperture to consider a full array of relevant threats and considerations, not only to address identifiable, material, concrete national security risks directly tied to actionable threats articulated in USG intelligence or vulnerability assessments, but also to consider other facets of resiliency including supply chain resiliency investments, U.S. competitiveness, availability and domestic manufacturing capacity, and workforce development.

Designing measures to advance and protect U.S. national security objectives without putting American competitiveness at risk. Lack of clarity in scope and process in any rulemaking, legislation, or other policy mechanism makes for an uncertain business environment and threatens the ability of companies to compete with foreign companies not subject to U.S. or similar foreign requirements. Overbroad policy approaches or approaches that duplicate or conflict with existing mechanisms, such as those embodied in the prior administration's *Executive Order on Securing the Information and Communications Technology Supply Chain* (*ICTS EO*), stifle U.S. innovation, technological leadership, and competitiveness. Members of this Committee should seize the opportunity to advance supply chain security policy approaches that are not only compatible with but drive global policymaking norms.

Collaborating closely with industry including leveraging industry resources and expertise. ITI's members understand we cannot tackle current and future supply chain challenges on our own, and that industry and government share responsibility to facilitate the global competitiveness of the U.S. technology sector and other critical sectors. Public-private partnerships and other multi-stakeholder approaches are essential to addressing supply chain resiliency and 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.

ITI has consistently encouraged ***U.S. policymakers to leverage the existing ICT SCRM Task Force as a focal point for public-private collaboration on supply chain security*.** The Task Force has brought together subject matter experts from the private sector and from across the USG, including multiple Commerce stakeholders, and has produced several actionable tools and other work products that can be used by industry and government to address supply chain security challenges, including related to information-sharing, threat modeling, procurement, vendor attestation and small and medium-sized businesses' unique needs. The administration should look to this established public-private mechanism for creative, actionable solutions, and should prioritize implementing and operationalizing Task Force products across the USG and incentivizing their promotion and uptake across the critical infrastructure community. I have been honored to serve as a co-chair of the Task Force on behalf of the IT sector since its inception, so I speak from personal experience in pointing out that the Task Force has focused on many of the same issues prioritized in USICA, and in recommending the Task Force as a good model for Commerce to emulate as it seeks to implement new programs such as the nascent Supply Chain Disruptions Task Force.

ITI has also advocated for inclusion of other key tenets in any strategic approach to supply chain resiliency, including **viewing supply chain risk management through the lens of trustworthiness** and **prioritizing bi-directional sharing of supply chain risk information.**

2. The Emerging U.S. Policy Approach to Supply Chain Resiliency as Reflected in *USICA/EFA* and the *100-Day Report*

ITI is pleased that both the Biden Administration and Congress have taken on board many of our policy recommendations in charting a broader, more holistic, and strategic approach to improving supply chain security and resiliency, as illustrated by both the *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth: 100-Day Reviews Under Executive Order 14017* (*100-day Report*) under the *ASC EO* and the supply chain provisions in *USICA*.

***ASC EO* and the 100-Day Report.** The *ASC EO* embraces the type of broader, holistic approach we have been advocating for the past few years, which balances important national security considerations with other considerations such as U.S. competitiveness. ITI particularly welcomed the *100-Day Report's* conclusions and recommendations on semiconductors, which tracked closely with several of ITI's recommendations offered in response to Commerce's RFI on the 100-day semiconductor review. We welcome the Biden Administration's commitment to building trusted, secure, and resilient supply chains, and we support its plan to realize that goal. Importantly, the administration outlined a clear vision to strengthen U.S. semiconductor leadership, including efforts to address research and development, increase manufacturing, and build a skilled workforce.

Support for CHIPS Funding. The 100-Day Review calls for $50 billion to fund the *CHIPS* and outlines additional steps to increase the domestic semiconductor manufacturing capacity and strengthen the U.S. technology workforce through STEM and training for semiconductor manufacturing. It also encourages enhanced cooperation with global partners and allies to ensure the stability of the global semiconductor supply chain. This forward-looking incentive will enhance economic competitiveness and bolster national security.

Request for a Supply Chain Resiliency Fund. We support the recommendation stemming from the 100-day Report which calls on Congress to fund the Supply Chain Resiliency Program proposed under the *Endless Frontiers Act* (*EFA)*, a part of *USICA*. This program, which requires close collaboration with the private sector, would help to formalize the ongoing activities taking place under the *ASC EO*, which are imperative to strengthening supply chain resiliency. While we appreciate the effort to provide needed liability protections to spur the sharing of supply chain risk information (SCRI) as part of the program, we also believe these protections could be further strengthened, as further articulated below.

Supply Chain Disruptions Task Force. We welcome the administration's plan to work with industry to develop a coordinated, streamlined, and holistic long-term approach to address semiconductor supply chain issues in a coordinated and holistic manner. The ICT SCRM Task Force provides a preeminent model in this regard, and we recommend synchronizing the efforts of this newly proposed Task Force with it to avoid duplication and leverage potential synergies that may result.

Collaboration on the Year-Long ICT Assessment. As the administration undertakes the longer-term assessment of the ICT industrial base, we continue to encourage close collaboration with the private sector to understand how it views the ICT supply chain, what it views as critical, where it sees gaps, and how government can best provide support. The ICT SCRM Task Force has been pleased to assist in the early stages of this assessment, as further explained below.

USICA/EFA Supply Chain Provisions. As stated previously, ITI commended the Senate's passage of USICA as providing a much-needed prioritization and expansion of critical investments in research, development, and technological advancement, including in the critical areas of semiconductor manufacturing, and addressing supply chain resiliency more broadly. A few key provisions include:

Emergency Appropriations for CHIPS and ORAN Funding. The emergency appropriations to fund provisions within *CHIPS* and the *Utilizing Strategic Allied Telecommunications Act* are imperative to maintaining a competitive edge in two technology areas key to U.S. leadership. As such, we are very supportive of the emergency appropriations, which provide an additional $52 billion to fund the semiconductor programs outlined in the FY2021 NDAA, and $1.5 billion to fund the Public Wireless Supply Chain Innovation Fund, which will help to support R&D for open architecture, software-based networks – technologies which the United States could leverage to address challenges related to vendor diversity that have emerged in recent years.

Commerce Supply Chain Resiliency Program. We welcome the proposal to develop a Supply Chain Resiliency Program housed in the Department of Commerce. As has been reiterated throughout the testimony thus far, there is a need for a more streamlined, coordinated approach to supply chain activities and this program would ideally help to achieve that objective. That being said, some of the activities listed under the purview of the Supply Chain Resiliency Program are already being undertaken pursuant to the *ASC EO*, though we appreciate that this program would formalize the review process called for there on a perpetual basis. We are further supportive that the program explicitly includes participation of the private sector in identifying and mitigating supply chain gaps. We also appreciate of the inclusion of liability protections to spur voluntary sharing of SCRI similar to those provided through DHS' Protected Critical Infrastructure Program (PCII), though as explicated below we believe those protections could be further strengthened. To effectively implement this program alongside all the other programs the Commerce Department is currently tasked with implementing, it needs to be appropriately resourced.

Investments in Manufacturing USA and Manufacturing Extension Partnership. We appreciate that the *EFA* would seek to quadruple the Manufacturing Extension Partnership program, including adding a specific track for cybersecurity and workforce development. This program has been helpful to manufacturers seeking to grow and we believe sustained funding will continue to help improve supply chain resiliency and U.S. competitiveness. Similarly, we appreciate that additional funding is provided for the Manufacturing USA program, aimed at supporting U.S. leadership in advanced manufacturing through this robust public-private partnership mechanism, another area that will be key to supporting supply chain resiliency.

Regional Technology Hubs. Although not strictly a supply chain provision, we welcome funding for the regional technology hubs, which will help increase the geographic diversity of supply chains across the U.S. Such hubs will support innovation, especially among smaller players across the United States, and spur additional workforce development and commercialization activities.

3. Commerce's Increasingly Important Supply Chain Policy Role and Implementation Track Record to Date

Commerce, as the federal steward of U.S. economic growth, competitiveness, job creation, and opportunity, is a key USG partner to ITI, the tech sector, and industry writ large. Commerce thus must play a central role in helping to make the ICT and other critical supply chains more resilient and secure. However, it cannot and should not be expected to do so alone or in an uncoordinated or ad hoc manner; rather it should continue to leverage its historical role as a convener and partner to industry and should also work closely with interagency partners to solidify the emerging U.S. policy approach to supply chain resiliency, as explained in the previous section.

However, it is important to view the new responsibilities the White House and Senate have proposed adding to Commerce's plate in the context of what has already been a significantly expanded role for Commerce in supply chain security and resiliency during the previous administration.

Commerce's Implementation Track Record for Supply Chain Policies and Programs Launched During the Prior Administration. Commerce is currently implementing several supply chain policy activities, rules, programs, and initiatives, including many launched during the last administration. The most significant of these include the following:

ICTS EO Interim Final Rule (IFR) and Licensing Process. Commerce bears primary responsibility for implementing the previous administration's ICTS EO, including taskings to finalize an IFR impacting a wide array of commercial ICTS transactions and to establish a new licensing or pre-clearance process applicable to a similarly large number of transactions. At present, the IFR provides the U.S. Secretary of Commerce (Secretary) with broad authority to review practically every single ICTS transaction with any nexus to an identified "foreign adversary," and casts a cloud of uncertainty over all other ICTS transactions given the list of named foreign adversaries could change at any time. When combined with the Secretary's additional power to block and unwind deals and the absence of an established, effective voluntary pre-clearance/licensing process (which Commerce has been delayed in developing or implementing), the fact that the broad IFR is "live" creates immense uncertainty in the business community that will result in an unnecessary, chilling effect on innovation and commerce. Commerce's responsibility for implementing these broad authorities under the ICTS EO alone raises significant questions regarding whether it has the resources or capacity to implement several new contemplated supply chain resiliency programs on top of this broad multilayered rule. **The implementation status of the IFR and the licensing program are uncertain at this time.**

Establishing a Process to Review Transactions Including Those Involving Chinese Apps. Although technically part and parcel of the ICTS IFR, as we understand it Commerce had separately been working on developing a meaningful transaction review process that would have also subsumed multiple other prior administration EOs directed at Chinese apps. While some of those EOs have been withdrawn by the Biden administration (see below), there remains a need for Commerce to develop a meaningful process for reviewing ICTS transactions. **The implementation status of Commerce's transaction review process is uncertain at this time.**

IAAS EO. The Commerce Department is currently tasked with implementing portions of the previous administration's *Executive Order on Taking Additional Steps to Address the National*

Emergency with Respect to Significant Malicious Cyber-Enabled Activities (IaaS EO), including promulgating regulations for identity verification of foreign account holders and regulations that enables the Secretary, in conjunction with other agencies, to require IaaS providers to take "special measures" blocking them from doing business in certain foreign jurisdictions or with foreign persons identified to be engaged in patterns of conduct allowing for the use of IaaS products in malicious cyber-enabled activities. **The two sets of regulations required to be promulgated by Commerce pursuant to the IaaS EO, whose authorities overlap in some respects with the ICTS EO, are not due until next week, while implementation of a third section of the EO is delayed.**

NDAA 2021 Provisions. Commerce is responsible for establishing the *CHIPS* grant program pursuant to section 9902 of the 2021 NDAA and the National Semiconductor Technology Center (NSTC) pursuant to section 9906, as well as for conducting a "Study on Status of Microelectronics Technologies in the United States" pursuant to section 9904. As stated elsewhere in my testimony, ITI encourages full funding of the *CHIPS* grant program and additionally suggests that efficient implementation of the NSTC by Commerce can leverage existing, proven industry ecosystems for semiconductor R&D where there are strong track records of innovation. The implementation status of the *CHIPS* grant program is pending funding via the emergency appropriations in *USICA*.

Additionally, although not directly related to supply chain resiliency, it is notable that, over the past few years, Commerce (specifically BIS) has been tasked with **significantly expanding the export controls system to emerging and foundational technologies** via implementation of ECRA, and **BIS has also been called upon to make numerous additions to the Entity List**. All this increased activity, while certainly justifiable for national security reasons, has also had an undeniable impact on the ability of Commerce/BIS to devote resources to the implementation of supply chain resiliency initiatives.

The unclear, and in many instances delayed, implementation status of numerous of the above-listed items helps to underscore the volume of supply chain resiliency and security responsibilities Commerce has accumulated and the resulting resource challenges it faces.

Commerce's Implementation Track Record for Supply Chain Policies and Programs Launched During the Current Administration. Commerce has more recently been charged with implementing several supply chain policy activities, rules, programs, and initiatives by the current White House, layered on top of all the activities stemming from the previous Administration. The most significant of these include the following:

ASC EO. The *ASC EO* gave Commerce two significant taskings: first, to conduct a 100-day review of the critical semiconductor supply chain and submit a report to the White House; and second, to lead a year-long comprehensive review (with DHS) and submit a report on supply chains for critical sectors and subsectors of the ICT industrial base, including the industrial base for the development of ICT software, data, and associated services." Because the ICT SCRM Task Force was asked by DHS and Commerce to help in the initial scoping of this review, I am confident in stating based on the work thus far that Commerce and DHS/CISA will both be required to expend significant additional resources to complete the *ASC EO* tasking over the next several months. I commend Commerce for its work in completing the 100-day review and for its initial outreach and partnership with the ICT SCRM Task Force on scoping the initial work for the year-long assessment and report.

EO on Protecting Americans Sensitive Data from Foreign Adversaries. This EO withdrew multiple EOs issued under the prior Administration banning transactions with certain Chinese apps in favor of a more process driven approach aligned with the regulatory regime required by the *ICTS EO*. It calls on Commerce to issue reports and evaluate on a continuing basis transactions involving connected software applications that may pose an undue risk of sabotage or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of ICT or services in the United States (amongst other things). **The implementation status of this EO and how it practically relates to the implementation of several of the above articulated taskings is unclear.**

Executive Order on Improving the Nation's Cybersecurity (Cyber EO). Commerce, particularly through the National Institute of Standards and Technology (NIST) and NTIA, also has a primary role in implementing section 4 of the new *Cyber EO* pertaining to strengthening the software supply chain. NIST has been tasked with identifying standards and best practices for the software supply chain, defining critical software, recommending minimum standards for source code testing, and initiating pilot programs related to IoT devices and software development practices. NTIA has been tasked with publishing minimum elements for a software bill of materials (SBOM), and it is noteworthy that NTIA has previously devoted a significant amount of resources over the past two years to running a multistakeholder process to conduct foundational work on SBOM.

It bears emphasizing that Commerce was responsible for all the above taskings even before the implementation of any potential *USICA/EFA* mandates or funding programs, should the bill pass the House and be signed into law. There are significant, legitimate questions that should be asked including: How do the above Commerce taskings relating to supply chain resiliency and security fit together? Does Commerce have sufficient resources and expertise to implement all these tasking simultaneously? And which bureau, office or other entity within Commerce is best equipped to lead and drive a coherent and coordinated approach to implementing supply chain resiliency across Commerce's many taskings?

4. Recommendations for Effective Implementation of Supply Chain Resiliency Policy

My testimony thus far helps to illustrate the substantial amount of progress that has been made by the Biden Administration and Congress to identify problems regarding the resiliency of key supply chains and craft sound policies to address these issues. However, such progress will not necessarily translate into effective implementation of those policies by Commerce and other federal stakeholders, particularly given the existing array of taskings Commerce is already implementing. Below I offer recommendations intended to help position Commerce and other relevant federal stakeholders for success in implementing the various emerging planks of U.S. supply chain resiliency policy, along with Commerce's many ongoing holdover responsibilities in this area.

Commerce should develop and articulate a strategic, coordinated plan for implementing its numerous supply chain taskings. As mentioned earlier in my testimony, ITI has consistently advocated for a centrally coordinated and holistic USG-wide approach to supply chain resiliency and security policymaking. Given the volume of supply chain taskings that have been layered upon Commerce by successive administrations as well as the new responsibilities contemplated by USICA, a coordinated, holistic, and strategic approach within Commerce is also clearly necessary to effectively implement its numerous supply chain taskings. Commerce is the preeminent federal stakeholder equipped to balance important U.S. competitiveness and economic interests with national security. Two key features of a strategic approach to achieve this balance should include identifying and empowering a specific entity within Commerce to lead and coordinate this work and ensuring that Commerce does not attempt to do all this work itself. Rather, Commerce should prioritize working with industry and other federal partners to create synergies and stretch scarce resources.

Congress should ensure that Commerce has adequate resources to effectively implement supply chain resiliency policy, including fully funding *CHIPS* and providing Incentives to enhance the domestic semiconductor ecosystem. ITI encourages the USG to provide meaningful incentives to increase domestic semiconductor manufacturing capacity of both leading edge and mature node semiconductors and to increase semiconductor R&D funding and prototyping. We encourage the U.S. House of Representatives to follow the Senate's lead and provide robust funding for *CHIPS* at the $50 billion level included in the 100-Day Report and Senate passed *USICA*, without distorting the incentives or the semiconductor market by favoring some sectors or applications over others, as a fundamental first step to boost the domestic semiconductor supply chain. These efforts should remain open to all multi-national chip manufacturers that meet the standards and guidelines set forth in *CHIPS*. Beyond that, it is imperative that Commerce is adequately resourced – in terms of both funding and staff – to carry out the full slate of supply chain resiliency policy activities identified above.

Commerce should prioritize close coordination with industry, including by leveraging existing partnerships, information sharing programs and innovation ecosystems. Policymakers and companies each have important and distinct roles to play in implementing supply chain resiliency. The USG has information that companies do not have about national security threats, whereas companies have information that governments do not have about their network operations and how they detect, manage, and defend against risks to data, systems, networks, and supply chains. Both policymakers and industry should communicate regularly and robustly about relevant risks (consistent with limitations relating to classified information and business confidentiality), including through opportunities for industry input in regulatory rulemaking processes, public-private task forces and other collaborative mechanisms, and informal relationships between policymakers and companies. As I stated earlier, the ICT SCRM Task Force provides an excellent model of public-private collaboration on supply chain matters that Commerce can draw inspiration from as it helps to launch the new Supply Chain Disruptions Task Force, which we urge Commerce to synchronize with the ICT SCRM Task Force.

Congress should ensure adequate liability protections to promote and incentivize the sharing of supply chain risk information. We appreciate the attention of the Senate Commerce Committee to include liability protections as part of USICA's supply chain resiliency fund to spur much needed voluntary sharing of SCRI. Increased information-sharing regarding risks related to suppliers and other aspects of the ICT supply chain can help both the government and industry to identify and mitigate supply chain risks. Currently, companies face challenges in sharing supplier risk information. This includes the legal risk of sharing potentially derogatory information about a supplier, the administrative barriers for federal personnel to share detailed, actionable information with individuals who do not hold clearances, and instances where the Federal government withholds vulnerability disclosures for offensive purposes. The ICT SCRM Task Force has developed a legislative proposal that would amend CISA 2015 to provide liability protections for companies that share SCRI information in good faith. This is a superior approach to the proposed extension of certain PCII protections in the Senate-passed USICA for several reasons. Most notably the PCII liability protections may not extend to industry-industry sharing of SCRI (which is much needed for companies to share information across their supply chains) and PCII may not preclude all regulatory uses of shared SCRI. Further, the PCII sections of USICA would not preclude potentially expensive lawsuits (because the provisions do not result in an automatic dismissal of lawsuits as does CISA 2015). Finally, PCII comes with heavy administrative burdens (including that companies need to apply to be part of the PCII program, be approved by DHS, and mark all covered materials), whereas CISA 2015 protections are automatically conferred to all shared information.

Commerce should focus the scope of the ICTS EO to ensure that covered transactions are prioritized and targeted according to discrete national security risks. In its current form, the ICTS EO and associated rulemakings will not only have potentially devastating effects on U.S. competitiveness and innovation, casting a cloud of uncertainty over almost all ICTS transactions with foreign entities, with limited benefit to ICTS security, but because the current scope of the ICTS EO and IFR remain so broad, implementation “as-is” will also sap a disproportionate amount of Commerce resources. We agree that supply chain security is imperative to facilitating trust, but the ICTS EO in its current state does not achieve those objectives, in large part because it focuses on risks associated with foreign adversaries to the exclusion of other risk-based considerations. Therefore, revising the EO and the scope of its rulemaking to ensure it is targeted at identifying and managing the greatest risks would allow U.S. companies to conduct global business with certainty, thus improving competitiveness and allowing for continued innovation across borders, while also freeing up otherwise limited Commerce resources.

Commerce and other USG Stakeholders should deepen engagement with international partners and pursue a coordinated approach to supply chain resiliency. Global ICT SCRM challenges ultimately call for globally scalable solutions, and we encourage the USG to collaborate with international partners and allies on supply chain resiliency issues to further common approaches to technology-related national and economic security risks – including through promotion of global, consensus-based, industry-led standards. For example, ITI welcomes the recent establishment of the U.S.-EU Trade and Technology Council as providing an opportunity to strengthen engagement and cooperation between the U.S. and EU on semiconductor and other strategic supply chains by conducting joint supply chain reviews to identify collaborative actions to improve resilience across semiconductor and other strategic supply chains.

Conclusion

Members of the Committee, ITI and our member companies are pleased you are examining how best to implement supply chain resiliency.

The USG has an unprecedented opportunity to lead on supply chain resiliency policy, and to do so it must work collectively, via public-private collaboration and across the federal government, both domestically and on the global stage. Commerce is appropriately at the center of this effort, but to succeed in implementing the many critical programs, rules and other taskings addressed in my testimony it must adopt a holistic, coordinated approach, exhibit strong leadership, embrace partnerships across industry and government, and be well-resourced and committed to the task.

ITI stands ready to provide you with any additional input and assistance in our collaborative efforts to develop policy approaches to supply chain resiliency 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 Chair, Ranking Member, and Members of the Committee for inviting me to testify today and for your interest in and examination of this important issue. I look forward to your questions.

Thank you.