ITI Promoting Innovation Worldwide

November 4, 2021

Mr. Matthew Borman
Deputy Assistant Secretary for Export Administration
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

RE: ITI Comments Responding to Bureau of Industry and Security Request for Public Comments on Risks in the Information and Communications Technology Supply Chain (RIN #0694-XC07; Docket No. 210910-0181)

Dear Mr. Borman:

The Information Technology Industry Council (ITI) appreciates the opportunity to provide a response to the U.S. Commerce Department's *Request for Public Comments on Risks in the ICT Supply Chain* (the RFC), pursuant to Executive Order 14017.

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.

Most of ITI's members service the global market via complex supply chains built over decades in which technology is developed 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 and making more resilient global information and communications technology (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 industries 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.

Of paramount importance to ITI and its member companies is our shared commitment to address risks to global ICT supply chains and national security more broadly. We believe government and industry must work together to achieve the trusted, secure, and reliable global ICT supply chain that is essential for protecting national and economic security and an indispensable foundation for supporting innovation and economic growth.

In the course of its review and its efforts to develop a whole-of-government strategy to improve ICT supply chain security and resiliency, we encourage the USG to consider both short-term and long-term efforts to foster a more robust U.S. and allied electronics ecosystem. Indeed, improvements will not happen overnight and will require strategic, long-term investments.

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

As such, we welcome the opportunity to provide input on several of the questions raised in the RFC, as well as offer policy recommendations around how to strengthen the resilience of global ICT supply chains.

Below, we offer an Executive Summary of our policy recommendations, followed by answers to discrete questions posed in the RFI.

- **Continue to build and leverage robust public-private partnerships to address ICT supply chain challenges.** ITI encourages the Administration to work with industry to develop a coherent, streamlined, and effective long-term approach to address ICT supply chain issues in a coordinated and holistic manner. The U.S. Department of Homeland Security (DHS) Supply Chain Risk Management Task Force provides a successful model.
- **Strengthen the technology workforce and develop advanced manufacturing capabilities across the ICT industrial base.** Policymakers should seek to increase funding for science, technology, engineering, and mathematics (STEM) and computer science education, advance legislative proposals for immigration reforms, and adopt other measures that help prepare the domestic workforce and attract the best talent from around the world to complement the U.S. workforce. This will help to administer advanced manufacturing across the ICT industrial base.
- **Enhance cooperation with global partners.** ITI supports increased bilateral, regional, and multilateral engagement with partner economies to deepen trade and investment relationships, including efforts to organize tech-sector specific dialogues, increase digital trade partnerships, enhance regulatory compatibility and reduce barriers to trade**.**
- **Make investing in critical technologies a national priority.** ITI encourages the USG to incentivize the construction of new and modernized manufacturing facilities and invest in research capabilities and elevate such investment to a national priority.
- **Avoid the wholesale repatriation of ICT supply chains.** Policymakers should seek to leverage existing global ICT supply chains to manage risks associated with concentration of manufacturing production and enable diversification, focusing investment on certain paramount capabilities as opposed to seeking to move entire ICT supply chains back to the United States.
- **Move quickly to fund the CHIPS for America Act.** ITI encourages Congress to take prompt action to fund the "Creating Helpful Incentives for the Production of Semiconductors" (CHIPS) for America Act and enact a strengthened version of the "Facilitating American Built Semiconductors" (FABS) Act to include an investment tax credit for both design and manufacturing.
- **Develop investment tax credits similar to those offered in the FABS Act for other ICT components and/or final ICT assembly.** ITI supports developing tax credits similar to those offered within the FABS Act for discrete or critical ICT products to promote manufacturing in the United States.
- **Address negative impacts of tariffs, including China Section 301.** Policymakers should consider developing an exemption process that allows for the reduction and/or removal of tariffs that negatively impact the ability of U.S. producers to reliably develop ICT products. We also encourage continued engagement with Chinese counterparts to develop a schedule to roll back and work to address ongoing trade barriers.
- **Streamline supply chain security policymaking activity.** Given the patchwork of existing supply chain security policy measures and work being undertaken across the federal government, ITI encourages the USG to streamline these activities. One way to do this

would be via designating a lead agency responsible for supply chain security risk management.

- **Ensure the introduction of new domestic preferences in USG procurement does not undermine the efforts being taken under EO 14017 to promote the resiliency and benefits associated with global ICT supply chains.** Overly restrictive U.S. federal procurement requirements will undermine and limit the ability of companies to participate in the global commercial and foreign government procurement marketplaces and hamper U.S. competitiveness.

I. Policy Recommendations

(ix) Policy recommendations or suggested action to ensure a resilient supply chain for the ICT industrial base

The RFC asks for policy recommendations to ensure a resilient ICT supply chain. Many of the recommendations we put forth in our response to the initial RFC on Risks in the Semiconductor Supply Chain, as well as the DOD RFC, remain relevant and applicable to the ICT industrial base more broadly.[1] We urge the Commerce Department to consider these suggestions as it seeks to devise a strategy to facilitate resilient ICT supply chains.

Continue to build and leverage robust public-private partnerships to address ICT supply chain challenges. Public-private partnerships are critical to fostering supply chain resilience and addressing challenges that may emerge. The U.S. government should leverage the existing ICT Supply Chain Risk Management Task Force as a focal point for public-private collaboration on supply chain security and resiliency issues. Policymakers should work with the Task Force leadership to develop a strategic plan to establish long-term support for the Task Force as a venue to co-develop solutions with industry to the nation's most pressing supply chain security, risk management and resiliency challenges. The Task Force has brought together subject matter experts from the private sector and from across the U.S. government and has produced several actionable tools and other work products that can be used by industry and government to address supply chain security and risk management challenges, including related to information sharing, threat modeling, procurement, and vendor attestation. Addressing supply chain security threats requires a holistic approach and the Administration should look first to this established public-private mechanism for creative, actionable solutions, and should prioritize implementing and operationalizing Task Force products across the U.S. government and incentivizing their promotion and uptake across the critical infrastructure community. Additionally, we urge the Administration to foster tighter coordination between and synchronize the efforts of the Supply Chain Disruptions Task Force, launched pursuant to the 100-Day Report called for by EO 14107, and the ICT SCRM Task Force.[2]

---

[1] ITI Submission to Risks in the Semiconductor Manufacturing and Advanced Packaging Supply Chain RFC. Available here: https://www.itic.org/documents/supply-chain/ITICommentsonSemiconductorSupplyChainRFCFinalSubmission4-5-21.pdf and ITI Response to DOD RFC on Supply Chain Assurance. Available here: https://www.itic.org/documents/supply-chain/ITIResponsetoDoDRFConSupplyChainAssurance.pdf

[2] Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth, 100-Day Reviews under Executive Order 14107, June 2021. Available here: https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf

Strengthen the technology workforce and develop advanced manufacturing capabilities across the ICT industrial base. The production of critical ICT components requires workers with highly specialized skills, including data analytics skills, technical equipment/operational skills, digital tooling skills, programming and coding sills, among many others.[3] More broadly speaking, developing advanced manufacturing capabilities across the industrial base is essential to sustaining competitive advantages across a wider ecosystem of products. Advanced manufacturing also relies on the integration of emerging technologies, such as artificial intelligence (AI), into various elements of the production process. Notwithstanding advances in technology and automation, the United States will continue to rely on a robust, highly trained, and skilled domestic workforce. The United States must therefore prioritize building and maintaining its domestic workforce by ensuring a steady talent pool with the necessary skills including advanced manufacturing and software engineering needed to meet future demand. Policymakers should support significant funding for science, technology, engineering, and mathematics (STEM) and computer science education, including technical training and new advanced hardware for teachers, expanded access to high-quality instructional materials and rigorous STEM and computer science coursework for students from underserved communities, hands-on practical experience for students, and effective regional partnerships.

Moreover, policymakers must ensure that all students have access to high-caliber STEM and computer science education, including underrepresented minorities and girls. It is also imperative to support increased funding and focus on training/upskilling programs in STEM and computer science through partnerships and other initiatives to facilitate placement of U.S. workers into digitally resilient jobs. Additionally, as manufacturing evolves so will its workforce. At the moment, manufacturing executives have identified the top skills necessary for the future advanced technological workforce to thrive, including technology/computer skills, digital skills, programming skills for robots/automation, data science and related AI skills, working with tools and an array of technology and critical thinking skills.

The Administration should also support solutions that allow companies to address their labor shortages and skills gaps today. Foreign talent is essential to the U.S. ICT industry. Consequently, policymakers should support immigration reform that successfully meets the demands of a globally competitive, digital economy by updating the U.S. employment-based green card the H-1B visa programs. For example, the Administration should support reforms that ensure that the number of available H-1B visas adjust to meet market demands; promote additional protections for nonimmigrant employees such as H-1B portability; provide funding for domestic STEM education and training programs; and support the H-4 work authorization visa program.

Enhance cooperation with global partners. The ICT supply chain is complex and global. Geographic diversification has become critical to the global competitiveness of U.S. firms, as it lowers costs, promotes efficiency and productivity, enables access to top global talent and growing customer bases, and helps mitigate supply chain risks. Companies often spend months if not years negotiating contracts with suppliers, planning manufacturing processes in line with rigorous quality controls, packaging and testing product security and efficiency, and providing customized services to clients around the world.

[3] Global Lighthouse Network: Insights from the Fourth Industrial Revolution. World Economic Forum. Available here: https://www.weforum.org/whitepapers/global-lighthouse-network-insights-from-the-forefront-of-the-fourth-industrial-revolution

The U.S. should work with partners and allies such as the EU, Japan, South Korea, Taiwan, and others in the Asia Pacific and the Americas to minimize damaging interruptions and ensure stability of the broader global ICT supply chain. Such efforts could include the convening of formal supply chain reviews with allies and building upon existing efforts to ensure that market access barriers do not present impediments to the efficient functioning and resiliency of global supply chains. This kind of engagement should seek to better enable firms to carefully calibrate their supply chains, maximize time-to-market, and account for other considerations that enable them to remain globally competitive. ITI strongly encourages the Administration to keep these global competitiveness considerations in mind and coordinate with foreign governments to ensure the stability of the global ICT supply chain, including by ensuring alignment on broader strategic objectives. Forums like the U.S.- Mexico High-Level Economic Dialogue, the U.S.-EU Trade and Technology Council, and the Quad should all be leveraged to foster dialogue amongst global partners and devise approaches to address identified challenges or risks.

Moreover, given the fact that several Asian economies are of central importance to evolving global ICT supply chains, their roles as growing hubs for trusted supply chain partners continue to be crucial. Alongside other structural factors, recent U.S.-China trade tensions have accelerated the diversification of supply chains in the Asia Pacific region, as companies have sought to move supply chains to ensure that they are not overly reliant on any one supplier or geography. ITI therefore supports increased bilateral, regional, and multilateral engagement with partner economies aimed at deepening trade and investment relationships and addressing any unintended trade barriers that restrict supply chain resilience. This engagement could include efforts to organize tech-sector specific dialogues, increase digital trade partnerships, enhance regulatory compatibility, and reduce barriers to trade.

Make investing in critical technologies a national priority. Ensuring America remains a leader in advanced high-tech manufacturing should be a core tenet of all USG policymaking aimed at strengthening supply chains. In the case of semiconductors, for example, while other governments have invested heavily to attract new semiconductor manufacturing and research facilities, the absence of comparable U.S. incentives has made the country less competitive, and America's share of global semiconductor manufacturing has steadily declined as a result. To be competitive and strengthen the resilience of critical supply chains, we believe the USG should incentivize the construction of new and modernized manufacturing facilities and invest in research capabilities.

ITI also encourages the United States to apply a principle of non-discrimination when incentivizing strategic investments. This will ensure that the United States remains a competitive investment destination for the world's most advanced and innovative technology solutions, from semiconductors to automobiles. In addition to bringing the most advanced technologies and associated jobs to the United States, a non-discriminatory approach reinforces the Biden Administration's priority of rebuilding relations with allies and partners and ensures that U.S. companies will get to benefit from similar programs abroad. For example, we are encouraged that the EU, Japan, South Korea, Taiwan, and Singapore have incentive programs for advanced manufacturing that allow for U.S. investors to participate equitably and fairly compared to domestic corporate applicants.

Avoid the wholesale re-shoring and repatriation of supply chains. By leveraging existing global supply chains, companies can invest resources in the R&D and advanced manufacturing programs

needed to support innovation in the United States. However, attempting to move the entire ICT supply chain to the United States, including for low-level inputs and components, would be cost-prohibitive, undermine U.S. global competitiveness, erode the trust of U.S. allies and partners, and is not practical or viable in many respects as discussed further below. It also comes into conflict with the value of comparative advantage in international trade and will undermine supply chain resiliency given the importance of diversification in building and maintaining resilience. Indeed, in light of the COVID-19 crisis, many of our member companies have taken steps to diversify production and their supply chains. Ensuring America remains a leader in advanced high-tech manufacturing should be the primary focus of U.S. trade and innovation policy. To that end, the Biden administration should focus instead on incentivizing certain baseline capability investments (such as the CHIPS Act and FABS Act for semiconductors & the fund proposed in the Build Back Better Framework under Section. 31401 Manufacturing for Supply Chain Resilience for other components) to address identified risks and vulnerabilities.

Move quickly to fund the CHIPS for America Act. ITI encourages Congress to take prompt action to fund the CHIPS Act and enact a strengthened version of the FABS Act to include an investment tax credit for both design and manufacturing. Semiconductors are essential to virtually all sectors of the economy – including aerospace, automobiles, communications, clean energy, information technology, and medical devices – and investments in this critical technology area is among the most strategic investments the United States can make in its future. Funding the CHIPS Act and enactment of a strengthened FABS Act will help the United States remain competitive by incentivizing semiconductor research, design, and manufacturing in the U.S., thereby strengthening the U.S. economy, national security, strategic partnerships, and overall ICT supply chain resilience.

> *(x) Any executive, legislative, regulatory, and policy changes, or any other actions, that would strengthen manufacturing or other necessary capabilities*

The RFC also seeks responses on policy changes that would strengthen manufacturing or other necessary capabilities necessary to support the ICT supply chain. We offer several considerations on this point.

Address the impacts of tariffs, including China Section 301. In addition to their direct impact on consumers, tariffs, such as those enacted following the China Section 301 investigation, impose significant economic costs on many parts and components that go into the ICT products under consideration in the RFC. At a time when the Administration is seeking to encourage the deployment of secure, trusted technology and ease supply chain constraints, the continued imposition of tariffs on key ICT goods and components causes unnecessary economic disruption and has a direct negative impact on U.S. competitiveness in key innovative technology sectors. The ability of ITI member companies to manufacture in America requires sourcing from a complex, interconnected global supply chain, which often includes China. But many imports subject to the China Section 301 tariffs do not represent high-value technology products – rather, they are necessary inputs into U.S.-made systems and are, in many cases, largely available only from Chinese sources. As noted in this submission, ITI member companies continue to take steps to diversify production and supply chains. But China remains an important source of many ICT components.

Therefore, beyond USTR's recent action to consider the extension of existing exclusions, we recommend that the USG consider an exemption process that allows for the reduction and/or removal of tariffs on other products that negatively impact the ability of U.S. producers to reliably

develop ICT products, particularly if those products are imported as part of the process of bringing manufacturing back to the United States. Furthermore, we continue to encourage U.S. engagement with Chinese counterparts to develop a schedule on which both sides can agree to roll back tariffs and advance implementation of the Economic and Trade Agreement between the United States and the People's Republic of China, as well as working toward developing solutions for ongoing trade barriers, including distortive government subsidization and restrictions of foreign cloud and financial services providers in China. Doing so would strengthen the ability of companies to manufacture in the United States by removing tariffs on those imported parts and components.

Consider developing investment tax credits similar to the FABS Act, but for other ICT manufacturing activity or final assembly of ICT products. This would spur an increase in domestic production by incentivizing manufacturing and research and development in the United States, which would in turn help to address supply chain vulnerabilities stemming from geographic concentration of manufacturing and final assembly.

> *(xi) Suggestions for improving the USG-wide effort to strengthen supply chains, including suggestions for coordinating actions with ongoing efforts that could be duplicative of EO 14017*

Over the past several years, uncoordinated approaches by the U.S. federal government to ICT supply chain risk management have resulted in a patchwork of overlapping, inconsistent and, in some cases, conflicting measures, including Executive Orders, agency actions, regulations and legislation. The net result has been a confusing supply chain security policy terrain that is increasingly difficult for companies to navigate, and which in many respects has not achieved the intended goal of improved supply chain security across the U.S. federal enterprise, critical infrastructure, and global private sector ICT supply chains. To this end, we released Principles for a Strategic Review of Supply Chain Security Policy earlier this year, which set forth recommendations for U.S. policymakers as they undertake a review of supply chains.[4] Several of the recommendations we made in that briefer are useful to reiterate in this context, especially to streamline ongoing supply chain security and broader resiliency activities.

We encourage the USG to streamline supply chain security policymaking activity. 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 policymakers 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 encourage the USG to designate a lead supply chain security risk management agency. To ensure the development of a coherent supply chain security policy, the U.S. Government should designate a lead supply chain security risk management agency and empower the National Cyber Director to coordinate these efforts, as ITI referenced in our Competitiveness Agenda.[5] Doing so will

[4] ITI Supply Chain Security Principles for a Strategic Review. Available here: https://www.itic.org/policy/ITI_SupplyChain_Principles2021.pdf

[5] Advancing Innovation to Make the U.S. More Globally Competitive: A Policy Memo for the Biden-Harris Administration and the 117th Congress. Available here: https://spark.adobe.com/page/FsDO0BYg1kIK7/

help to avoid duplication of efforts and ensure that efforts to address both federal and commercial supply chain security risks are complementary.

We encourage the USG to clearly differentiate how ongoing activities interrelate with each other. As the supply chain reviews continue, we urge the USG to clearly state how the respective activities interrelate with each other. We note that the RFC did not mention semiconductors, which are a fundamental part of the ICT supply chain, but which were also addressed in a previous RFC pursuant to EO 14107 and now in a simultaneous RFC, also related to EO 14107, seeking additional information. It is not clear how efforts on semiconductors will either be folded into the ongoing efforts to foster a more resilient ICT supply chain industrial base, or otherwise be addressed separately. In our view, any efforts to build up the ICT supply chain industrial base more broadly will need to consider the very real semiconductor supply chain challenges, but it is not clear from the RFC how these activities are related to each other, if at all, or how the outputs will be synthesized into a unified approach for addressing ICT supply chain resiliency challenges. As another example, new rules have been promulgated and are in ongoing development at the Commerce Department with regard to Securing the ICTS Supply Chain. Ensuring that all of these efforts are coordinated and consistent will help with developing an effective framework to manage risks related to the ICT supply chain.

We encourage the USG to remain in close contact with the FAR Council to ensure that the introduction of new domestic preferences in USG procurement does not undermine the efforts being taken under EO 14017 to promote the resiliency and benefits associated with global supply chains. ITI has already provided separate comments in response to Federal Acquisition Regulation (FAR): Amendments to the FAR Buy American Act (BAA) Requirements (FAR Case 2021-008) but wants to raise for Commerce's consideration the nexus between FAR Case 2021-008 and the rulemaking associated with EO 14017, followed by broader points from ITI's submission as many of them are relevant to the RFC's questions.[6] According to FAR Case 2021-008 as released on July 30, 2021, products and items identified through the quadrennial supply chain review instituted in EO 14017 as well as the National COVID Strategy would then undergo a subsequent assessment by the Office of Management and Budget (OMB) to determine a list of critical items or end products with critical components that would be subject to unique, item-specific price preferences for purposes of U.S. Government procurement.

ITI's comments in response to FAR Case 2021-008 requested greater clarity with regard to the treatment of items subject to the commercial information technology (IT) or commercially available off-the-shelf (COTS) exemptions that may be considered as critical products or contain critical components. The USG's identification of a product or component as critical does not alleviate the circumstances that led Congress to legislate an exception to BAA rules for commercial IT and the Office of Federal Procurement Policy to waive the component test for COTS items. Subsequent rulemaking to address the treatment of such items that meet either or both conditions should bear these circumstances and conclusions in mind. In our comments, we urged the FAR Council to defer any further rulemaking directed to critical products and components until the quadrennial critical supply chain review has been completed and a more robust policy prescription can be formulated.

[6] ITI comments responding to FAR Case 2021-008. Available here: https://www.regulations.gov/comment/FAR-2021-0008-0049.

More broadly, ITI appreciated the opportunity to submit comments to FAR Case 2021-008 and to participate in the public hearing on August 26, 2021. We strongly encouraged the FAR Council to continue conducting robust stakeholder engagement, and to establish sufficient procedural guardrails that will protect against potential politicization of the waiver review process. The global technology industry supports the U.S. Government's goal of ensuring reliable access to the best technologies and products, and the comments and concerns expressed in ITI's submission are shared in that spirit.

ITI is concerned that the imposition of new U.S. federal government procurement requirements without the benefit of robust stakeholder engagement would undoubtedly harm the U.S. Government's access to potentially the best available products, which may not be made in the United States at all. Such an impediment would have significant implications for the U.S. Government's ability to ensure reliable access to these technologies and the ongoing success of U.S. digital transformation efforts.

For example, the rapid increase in content thresholds may present a challenge to offerors to federal procurements as supply chains may not be adjusted to meet new thresholds as quickly as the proposed rule suggests, particularly given the current supply chain challenges globally. Additionally, increased content thresholds place an immediate administrative burden on offerors in ensuring their products and products from lower-tier suppliers continue to meet growing content thresholds, which brings an added cost to the offerors and detracts from efforts to provide best available products to meet pressing government needs. Given these inevitable effects, ITI encouraged the FAR Council to make the imposition of any new requirements measured, targeted, and gradual so U.S. interests are not inadvertently harmed.

ITI also expressed concerns that overly restrictive U.S. federal procurement requirements will undermine and limit the ability of companies to participate in the global commercial and foreign government procurement marketplaces. This impact will in turn disrupt the virtuous cycle of private-sector R&D investments made possible by revenues from sales of U.S. products to a diverse customer base in overseas markets. U.S. national security depends on continued U.S. technological leadership on a global scale. This leadership in turn drives U.S. innovation, job creation, and economic growth. Remaining at the cutting edge of developing and commercializing technologies will ensure they are available to the U.S. Government, private sector, and the defense industrial base. Given the desire of the Administration and Congress to ensure that U.S. companies remain among the most innovative and competitive in the world, a balanced and thorough review of these impacts is essential. The Department of Commerce should take into account these concerns as it works across the interagency to promulgate policy related to addressing risks in and improving the resiliency of the ICT supply chain.

II. Critical Goods and Materials & Manufacturing Capacity Required

(i) "Critical goods and materials" that underpin the ICT supply chain, including goods and raw materials currently defined under statute or regulations as "critical" as well as "other essential goods and materials" including "digital products" that underly the ICT supply chain

There are many elements that are foundational to the ICT supply chain products and services. Based on the scope of the ICT supply chain as laid out in the RFC, we offer some illustrative

examples of goods and materials that we consider to be critical. This list is not exhaustive but is demonstrative of the breadth of items that are key inputs into the ICT supply chain, and which may currently be at risk for several reasons outlined below.

Mature and Advanced Semiconductors/Integrated Circuits

In our response to BIS's RFC on Risks to the Semiconductor Supply Chain, we discussed how foundational semiconductors are to information and communications technology (ICT) products and services across our industry, products, and services, which in turn are integral to driving economic growth and innovation across most industries and sectors.[7] They are critical to many technologies that rely on a secure supply of chips, including AI, IoT, and others. Presently supply chains for these products face a variety of risks, including climate and environmental risks, geopolitical risks, regulatory risks, workforce challenges, and supply of rare earth elements. Given we addressed many of these risks in great depth in our prior response, we will not go into the same level of depth in this response. We point BIS to our response to that RFC, as well as our response to the ongoing BIS semiconductor survey.

Memory and Storage

Memory and storage are used in every IT system and in other industries outside of the ICT sector. As such, this hardware is essential to ICT products and services, including those listed in the RFC. While memory production is not facing significant backlogs, inputs like subsystem control integrated circuits are currently facing resiliency impacts, including a current shortage of these units. Additionally, about 70 percent of memory production is located in allied countries in East Asia, which presents further risks around concentration of supply.[8]

Displays (specifically LCDs)

Displays are needed in a variety of ICT products and beyond. They require driver integrated circuits to operate. See above section on semiconductors for additional information about the risks that supply chain is currently facing. Beyond that, there are few suppliers for displays and high capital costs associated with their manufacture, which may have a resiliency impact. In recent years, suppliers have been concentrated in China.

Rechargeable Batteries (lithium ion) & Adapters/Chargers

Lithium-ion batteries are present in many "end user devices" and "home devices" as scoped in the RFC. They are critical to the function of many of these devices, offering a power source for portable electronic devices. They also require cell separators and management ICs.

Adapters/chargers are also critical to most IT systems, as one is required per IT system or electronic device. Rare earth metals are incorporated into these products, which means if the gallium nitride

[7] ITI Submission to Risks in the Semiconductor Manufacturing and Advanced Packaging Supply Chain RFC. Available here: https://www.itic.org/documents/supply-chain/ITICommentsonSemiconductorSupplyChainRFCFinalSubmission4-5-21.pdf

[8] Strengthening the Global Semiconductor Supply Chain in an Uncertain Era. BCG & SIA. Available here: https://www.semiconductors.org/wp-content/uploads/2021/05/BCG-x-SIA-Strengthening-the-Global-Semiconductor-Value-Chain-April-2021_1.pdf

supply was interrupted or unavailable, for example, there would be an impact on the ability to produce and source these chargers.

Printed Circuit Boards

Again, PCBs are used in every electronic component. There are typically dozens in a typical IT system, including one "main" board and many smaller boards, and PCBs additionally present risks related to manufacturing and domestic production capability. Indeed, it is difficult to manufacture PCBs safely without producing toxic byproducts. There is also very little U.S. production capacity.

Rare earth elements

Other raw materials, including rare earth elements (REEs), are integral to the ICT supply chain and further analysis is necessary to fully assess areas of resilience impact. REEs are foundational to many ICT products and the availability of REEs has been a recurring issue in a variety of contexts. China, the leading producer of REEs, has already begun to restrict REE exports. China is also working to control the international sources of REEs for which China, the US, and other nations necessarily compete. To the extent specific REEs are not produced within the US, the risk to the US and the ICT sector is directly proportional to the impact of an insufficient supply of such REEs. Below is a non-exhaustive list of selected REEs that may impact ICT supply chain resilience.[9]

Component	Product	Country of origin
Gallium	Semiconductors, LED, solar cells	Mainly produced in China
Germanium	Fiber optics, solar cells	
Indium		Mainly produced in China; Korea
Rare Earth Elements (REEs)	Computer displays; LEDs	Disproportionate amount produced in China; also some in U.S. and Australia
Selenium	Photovoltaics	
Tantalum	Capacitors/sputtering targets	

Cloud Computing and other ICT Services

Another important aspect of the ICTS ecosystem and supply chain involves ICT services, including cloud computing services. However, given the fact that this aspect of the ecosystem is fairly broad, we recommend that Commerce/BIS and CISA explore cloud computing and other services separately, and focus this report specifically on ICT hardware and software.

(iii) Manufacturing, or other capabilities necessary to produce or supply the materials and services above, including emerging capabilities;

Manufacturing ICT products requires a host of components and products, including equipment for tooling and testing, which is highly automated and capital intensive. Additionally, manufacturing requires capabilities like advanced wastewater treatment, air filtering, high volumes of non-toxic

[9] See Dec 2020 UNCTAD report for additional information.

(e.g., water) and toxic or flammable (e.g., solvents) chemicals used in processing, and an extremely large and stable electricity supply – factories rarely use the existing civil power grid due to inadequate supply or inadequate quality of power (voltage fluctuations, etc.), and/or install significant power conditioning equipment and backup systems. As referenced on pages 2 and 4 above, manufacturing of critical ICT products also requires a highly skilled workforce, as does software development, so we further encourage the USG to focus on the development of such a workforce as foundational to addressing ICT supply chain resiliency challenges in the long term. Labor costs and facility costs also play a significant role in manufacturing.

III. Risk Assessment

(iv) Risks or contingencies that may disrupt the ICT supply chain (defense, intelligence, cyber, homeland security, health, climate, environmental, natural, market, economic, geopolitical, human-rights or forced-labor risks), as well as risks posed by a reliance on digital products that may be vulnerable to failure or exploitation and risks that may result from the failure to develop domestic capacity to manufacture/other capabilities

There are a wide variety of risks and contingencies that have the potential to disrupt the ICT supply chain, many which we alluded to in the prior section outlining illustrative examples of critical hardware and services. In considering the broad array of risks or contingencies that may disrupt the ICT supply chain, we encourage the Commerce Department to reference the reports developed by the ICT Supply Chain Risk Management Task Force Working Group 2 focused on Threat Evaluation, which identified a wide range of supplier-related threats in year one, and catalogued threats related to ICT products and services in year two. These reports may serve as a helpful resource to the Commerce Department as it undertakes its analysis of the semiconductor and advanced packaging supply chains.[10] Working Group 2 bucketed these threats into a series of threat categories related to the ICT supply chain, including suppliers, products, and services, and proposed mitigating measures to address identified threats.

We encourage the Commerce Department to consider all of the threat categories identified in the report, which looks at threats from a variety of vantage points and which all touch upon the risk of relying upon products that may be subject to failure and/or exploitation. The insertion of counterfeit parts, for example, could have a significant impact on products and services provided to downstream customers, especially if a trusted or qualified component is replaced with a counterfeit product from an untrusted or unqualified source. Such exploitation can result in several different outcomes, ranging from creating an unwanted function to inserting compromised components into organizational systems to embedding hardware or software threats into a product. Adversaries may also be able to leverage compromised components to launch an external attack on systems, gain unauthorized access to equipment or systems, or otherwise exploit such vulnerabilities to exfiltrate information and/or data.

[10] ICT Supply Chain Risk Management Task Force Threat Evaluation Working Group: Threat Scenarios. January 2021. https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v2.pdf

We also outline several other risks which generally impact all the categories referenced above.

Barriers to trade. The introduction of new restrictions or compliance requirements by either the U.S. government or other governments (e.g., export control requirements) can further increase costs and inject uncertainty into supply chains. For example, imposing new, restrictive controls on foundational or emerging technologies as a result of the Export Control Reform Act of 2018, including on key ICTS products, components, or software, could exacerbate current U.S. supply chain resiliency challenges by making it more difficult for companies to develop, assemble, or manufacture ICTS products overseas that are needed in the U.S. market. Beyond that, tariffs on ICT products have the potential to disrupt supply chains (and already are, as evidenced by the China Section 301 tariffs that are currently being applied to some ICT components).

We specifically draw Commerce's attention to the importance to U.S. supply chain resiliency of prohibiting the imposition of trade barriers to electronic transmissions. For more than two decades, all members of the World Trade Organization (WTO) have committed to the Moratorium on the Imposition of Customs Duties on Electronic Transmissions (Moratorium). The term "electronic transmissions" is not defined but is commonly held to encompass a wide variety of ICT products and services ranging from software, emails, and text messages to digital music, movies, and videogames. To date, no country has imposed tariffs on electronic transmissions, a testament to the success of the Moratorium, the broad recognition of the economic damage the application of customs duties on electronic transmissions would yield in terms of absolute costs and heightened uncertainty, and the technical infeasibility of administering tariffs on electronic transmissions. However, in recent years, opposition to the renewal of the Moratorium has grown in the WTO, with some members hoping that a lapse of the Moratorium will provide them with new opportunities to generate customs revenue.

For ITI member companies, the Moratorium ensures their internal and external electronic transmissions can support efforts throughout global supply chains: researching, designing, and developing innovative technologies; negotiating contracts with suppliers; planning manufacturing processes in line with rigorous quality controls; packaging and testing product security and efficiency; and providing goods and services to clients around the world. It follows that the U.S. Government should prioritize the renewal of the Moratorium at the upcoming 12th WTO Ministerial Conference (MC12) as a means of shoring up the electronic transmissions that underpin the operation and resiliency of global supply chains. Moving forward, we welcome continued USG efforts to expand permanent prohibition of the imposition of customs duties on electronic transmissions.

Human capital gaps. Across the ICT supply chain there are human capital gaps holding the potential to disrupt the supply chain. Indeed, as we have mentioned in several areas throughout our submission, a highly skilled workforce is imperative to future technological advancement. At the moment, companies oftentimes utilize foreign talent to meet these needs. For example, although there are U.S.-based software developers, companies oftentimes also need to find workers with such skills outside of the United States. Additionally, gaps in STEM education and technical training exist demonstrating a need for additional training and upskilling programs in STEM fields and in computer science.

(v) The resilience and capacity of American ICT manufacturing supply chains to support national and economic security and emergency preparedness, including an assessment of:

(A) & (E) manufacturing capacity and gaps in manufacturing capabilities; location of key manufacturing and production assets, and risks posed by those locations

Manufacturing capacity in the United States for many ICT products is limited. Indeed, most manufacturing and packaging for high-volume microelectronics packaging and test capability for advanced semiconductors and other ICT products more broadly takes place in East Asia, a region that presents geopolitical risks. That being said, ITI member companies continue to operate advanced IT manufacturing across the United States as well.

However, we do see a gap in the United States in the lack of ability to assemble final products, combined with the lack of a local supplier ecosystem. Hence, at present actual manufacturing capacity is limited in the United States. It is our view that there needs to be a more systematic approach to improving quality advanced manufacturing in the United States.

(C) information and cybersecurity practices and standards of the ICT sector that may address identified risks, with a particular interest in comments related to validation standards of component and software integrity, standards and practices that help to ensure availability and integrity of software delivery and maintenance, and security controls during the manufacturing phase of ICT hardware and components;

This specific set of risks seem more specific to security as opposed to resiliency, which appears to be the intent of the rest of the *America's Supply Chains Executive Order*. As such, we encourage Commerce to address specific issues related to software supply chain security via mechanisms laid out in the *Executive Order on Improving the Nation's Cybersecurity (EO 14028)*, which directs NIST and other agencies to develop a set of guidelines that incorporate standards and best practices to enhance software supply chain security, including around employing automated tools to maintain trusted source code supply chains, providing artifacts that demonstrate conformity, maintaining accurate and up-to-date data, provenance, and controls on software components, and providing a software bill of materials where appropriate. We believe this process and associated RFIs are better suited to address this specific set of risks and would encourage the Commerce Department to utilize these processes to inform a broader holistic strategy to address these risks, as opposed to tackling them under this Executive Order. Overall, however, Commerce should seek to leverage existing industry-lead, globally recognized cybersecurity standards, as opposed to creating a new regime. Many of the challenges mentioned above are already addressed by existing standards and frameworks, and the issue is more about accelerating widespread adoption of those standards, rather than creating new ones.

(F) exclusive or dominant supply of critical or essential goods from unfriendly nations;

As referenced in the above discussion of critical goods and materials, many ICT products are made with minerals or metals that are largely sourced from unfriendly or adversarial nations. For example, many rare earth metals are mined in China and cannot be sourced elsewhere.

With regard to software, it is worth noting that most software development undertaken in "countries of concern" occurs because of low costs of labor or physical proximity to hardware

manufacturing, as well as that most software is founded on open-source code, meaning that developers are located all over the world. This reality can, in turn, potentially impact the resilience of certain ICT services, including help desk services, DNS services, PKI encryption services, etc.

(G) availability of substitutes;

While substitutes may be available in some cases, it is important to consider that at the scale/quantity required to manufacture it is often incredibly difficult to source those substitutes outside of countries of concern.

(H) relevant workforce skills necessary to fulfill future workforce needs;

The production of critical ICT components requires workers with highly specialized skills. We elaborated on skills that are required for semiconductor design and manufacture in our prior submission. Similar skills are needed across the ICT sector and beyond, especially as technological adoption continues. Beyond that, developing and maintaining the advanced manufacturing capabilities required to bolster U.S. leadership in the production of critical technologies will require a highly trained and skilled domestic workforce. According to the World Economic Forum's *Future of Jobs* 2020 report, business leaders have cited challenges when hiring for data analysts and scientists, AI and machine learning specialists, and software and application developers.[11] It is thus clear that skills including data analytics, statistical programming, and computer networking will be necessary to support a successful future workforce. In addition to skills needed for advanced ICT design and manufacturing, skills also are needed to address quality control and potential engineering issues related to lower-level, upstream ICT products that are integrated into more advanced US products. US innovators and manufacturers must have the necessary engineering skills to address quality and engineering issues in order to manage supply chain expectations. There is also a need to for skills that support jobs on and off the manufacturing floor, including technical skills to work the manufacturing line, in inventory control management, as well as in program, process, and product management, procurement, and supply chain management.

(I) need for R&D to sustain leadership in services or critical goods/materials;

As we mention in our policy recommendations, there is a critical need for significant R&D to sustain U.S. leadership in critical technologies and services. Sustained investment in R&D for both critical and foundational technologies will be required to bolster the United States' ability to lead in the ICT sector. As such, we support funding such as that envisioned in the CHIPS Act and the Supply Chain Resiliency Fund.

(J) role of transportation and transmission systems;

Transportation and transmission systems play an integral role in the resiliency of supply chains. For example, logistics and warehousing are vital to global ICT supply chains, and include transport/shipping of components, subsystems, and goods across the global supply chain. Some materials may pass through 10-20 countries (or more) from extraction to end customer. This can create risks, particularly because the longer the supply chain, the more cost and complexity to

[11] The Future of Jobs Report 2020. World Economic Forum. Available here: https://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf

source products into the US market. During the pandemic, transportation costs increased significantly (2-3x), which will impact the ICT market for years to come.

Global ICT supply chains can also potentially be put at risk by, e.g., a ship blocking the Suez Canal or a labor strike at a key port (Hong Kong; Singapore; Long Beach, CA), especially given the limited domestic sources for materials to enable and feed into some of the critical aspects of the ICT supply chain identified above. It is important to consider risks that are unanticipated as well as those that may be impacted by the legal environment, such as labor laws or laws and regulations in other areas.

Transmission systems also play an important role in facilitating global ICT supply chains as a reliable and resilient supply of energy, including electricity, is required for the manufacturing of various ICT components and products. It should also be noted that disruptions in electricity can broadly impact the functioning of ICT systems and the provision of various ICT services.

(K) risks posed by climate change;

Climate-related events are occurring at increasing scale and help to highlight that a globalized supply chain has become critical to managing these increasing risks. For example, the semiconductor industry was able to manage multiple COVID-19 outbreaks and natural disasters and actually produce and ship more semiconductor chips than it did prior to the pandemic. While these challenges did force some localized closures and production delays in places like Texas and Malaysia, production was able to continue elsewhere and allow for substantial increases in semiconductor manufacturing globally over the past two years. While we fully understand that there is a shortage of semiconductors, this largely has to do with unprecedented, pandemic-induced demand and would likely be much worse if it were not for the inherent resiliency of a globalized supply chain.

(vi) Allied and partner actions, including how those nations have defined/prioritized critical goods and avenues for international engagement

Allied and partner nations are also considering how to foster secure and resilient supply chains. As mentioned in our policy recommendations, continued engagement and collaboration with allied and partner nations is imperative to maintain a robust and resilient global ICT supply chain. For example, the European Commission has conducted reviews of six "strategic areas," which includes a list of 30 raw materials that are essential to those strategic areas.[12] Beyond those raw materials, the Commission has identified active pharmaceutical ingredients, lithium-ion batteries, hydrogen, semiconductors, and cloud and edge computing as other areas of strategic importance. It is worth noting that Europe did not identify the ICT supply chain as a whole as strategic but focused specifically on semiconductors and cloud and edge computing in the context of its review.

Australia has also undertaken a similar effort in response to supply chain challenges it faced during the COVID-19 pandemic. Under its Sovereign Manufacturing Capability Plan it plans to "safeguard access to critical products and build more resilient supply chains," and identified medicines,

[12] In-Depth Reviews of Strategic Areas for Europe's Interests. Available here: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy/depth-reviews-strategic-areas-europes-interests_en

agricultural production chemicals, and personal protective equipment as critical products that may be impacted by supply chain vulnerabilities.[13] The ICT sector/industrial base was not included in Australia's initial analysis.

We encourage the USG to continue its international collaboration, leveraging forums and dialogues to develop creative solutions to supply chain resiliency challenges. We referenced several of these forums in our policy recommendations above but reiterate the importance of working through the working groups established under the U.S.-EU Trade and Technology Council, the U.S.-Mexico High-Level Economic Dialogue, and the Quad, as well as establishing additional working groups or committees in other existing bilateral and multilateral mechanisms dedicated to fostering greater supply chain resiliency.

***

We appreciate the opportunity to provide feedback to the Commerce Department to inform the one-year ICT supply chain report it will provide to the White House. We believe that ICT supply chain resiliency can be enhanced through targeted policy measures aimed at incentivizing R&D, developing the domestic workforce, working with partners and allies, and streamlining supply chain security policymaking, among other things. We look forward to continuing to partner with the USG as it seeks to develop a whole-of-government approach to address supply chain security and resiliency issues. Please do not hesitate to contact us with any questions you may have about our submission.

Sincerely,

John S. Miller
Senior Vice President of Policy
and General Counsel

Courtney Lang
Senior Director of Policy

[13] Sovereign Manufacturing Capability Plan: Tranche 1. Available here: https://www.industry.gov.au/data-and-publications/sovereign-manufacturing-capability-plan-tranche-1