Before the

BUREAU OF INDUSTRY AND SECURITY

Washington, DC 20230

In the Matter of

	)	
Notice of Request for Public Comments on Risks	)	Docket No. 210910-0181
in the Information Communications Technology	)	RIN- 0694-XC07
Supply Chain	)	
	)	

COMMENTS OF THE
TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Tom McGarry
Vice President, Standards

Colin Black Andrews
Senior Director, Government Affairs

Patrick Lozada
Director, Global Policy

TELECOMMUNICATIONS INDUSTRY
ASSOCIATION
1310 N. Courthouse Road
Suite 890
Arlington, VA 22201
(703) 907-7700

Filed: November 4, 2021

INTRODUCTION AND SUMMARY

The Telecommunications Industry Association ("TIA") appreciates the opportunity to provide input regarding Risks to the Information and Communications Technology ("ICT") supply chain.[1] TIA represents more than four hundred U.S. and global manufacturers and vendors of telecommunications equipment and services. In addition to engaging with government stakeholders, TIA is an ANSI-accredited Standards Development Organization, the administrator of the Mobile Equipment Identifier ("MEID") numbering system, and is the parent of QuestForum which manages TL9000 – the leading Quality Management System ("QMS") for the ICT industry. As such, understanding and mitigating risks to the ICT supply chain is central to our mission as an organization.

As a voice for the ICT supply chain, the work the Department of Commerce and specifically the Bureau of Industry and Security ("BIS") is doing through this notice and under the President's Executive Order on Securing America's Supply Chains[2] ("Supply Chain EO") is a top priority to our members. Specifically, TIA's comments will focus on the following issues in response to questions raised in the Notice:

- *Manufacturing or other needed capacities of the United States related to ICT design and manufacturing (v., A):*
    - Congress should act to fund the CHIPS Act and pass the tax incentives in the FABS Act. The Commerce Department should subsequently act to implement this funding in a way that is technology neutral and avoids preferencing specific end uses.

[1] Notice of the Request for Public Comments on Risks in the Information Communications Technology Supply Chain, Bureau of Industry and Security, Department of Commerce, Docket No. 210910-0181 (Sep. 20, 2021) ("Notice").

[2] Executive Order 13873, 84 Fed. Reg. 22689, Executive Order on Securing the Information and Communications technology and Services Supply Chain (May 15, 2019), (available at https://www.whitehouse.gov/presidential-actions/executiveorder-securing-information-communications-technology-services-supply-chain/).

  - The R&D tax credit should be clarified – either by the Treasury Department or by Congress – to include expenses related to standards development in order to support American leadership in ICT standards.

- *Information and cybersecurity practices and standards of the ICT sector (v., E):*

  - The government should support industry standards and best practices – and specifically TIA's SCS 9001 standard – as ways to enhance security and promote transparency in the ICT supply chain.

- *Workforce (v., X):*

  - U.S. government should support programs that allow employers to expand registered apprenticeships and associated technical instruction and certification costs.

  - Government should enact policies that bolster the capabilities of institutions of higher education and other institutions to ensure a diverse workforce capable of deploying fiber and 5G infrastructure for commercial mobile and fixed wireless networks.

  - Public-private partnerships with community colleges, universities, and other institutions to develop degrees and programs of study on broadband deployment and 5G training, should be expanded.

  - Immigration procedures for H1B and other high-skilled worker programs should be streamlined to ensure that innovative U.S. ICT companies can leverage a global talent pool.

- *Prioritization of "critical goods and materials" (viii)*

  - TIA believes that action to support the manufacturing of critical ICT products should be technology-neutral and avoid preferencing any method of connectivity.

- *Specific policy recommendations important for ensuring a resilient supply chain for the ICT industrial base (ix)*

  - BIS and the Department of Commerce should revisit the policy recommendations in the National Strategy to Secure 5G Implementation Plan that resulted from the extensive consultation with the ICT industry.

DISCUSSION

To provide useful feedback for BIS, TIA has provided our comments in a manner organized by each individual question raised in the Notice.

(v) resilience and capacity of American manufacturing supply chains, including ICT design, manufacturing, and distribution, and the industrial base—whether civilian or defense—of the United States to support national and economic security, information security, emergency preparedness, and the policy identified in section 1 of E.O. 14017, in the event any of the contingencies identified in paragraph (iv) above occurs, including an assessment of:

(A) manufacturing or other needed capacities of the United States related to ICT design and manufacturing of products and services, including the ability to modernize to meet future needs;

Given the impact of the current semiconductor shortage on the telecommunications sector and the foundational role chips play in supporting the broader manufacturing supply chain, there is a clear need to improve the manufacturing capacity for semiconductors in the United States. To that end, TIA supports funding for the Creating Helpful Incentives for Producing Semiconductors ("CHIPS") Act provisions of the 2021 National Defense Authorization Act ("NDAA") and the passage of the Facilitating American-Built Semiconductors ("FABS") Act tax credit.

Telecommunications is the single largest end user of semiconductors, making up 50% of all chip end uses.[3] Given the importance of ICT equipment in the daily lives of Americans and the impact this current shortage has had on getting ICT products into consumers' hands, the U.S.' current semiconductor manufacturing capacity does represent a potential vulnerability to the ICT supply chain. Funding the CHIPS Act and passing the FABS Act would represent a

[3] The White House, *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth: 100-Day Reviews under Executive Order 14017*, at page 25 (June 2021) (available at https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf).

significant step towards ensuring that the U.S. can continue to maintain and increase manufacturing capacity in this sector, which would result in a more resilient ICT supply chain.

Another important element of the ICT manufacturing ecosystem is the continued advancement of standards to promote interoperability and facilitate communication between components and devices from all manufacturers. While standards are important in nearly every sector of the economy, they are particularly important in the telecommunications sector where the basic function of ICT products relies on the ability of devices from different manufacturers to communicate with one another using common protocols and interfaces. Most key telecommunications standards – such as the 5G standards developed by the 3rd Generation Partnership Project ("3GPP") – are developed by the private sector.

The U.S. has traditionally played a leading role in developing such standards, however, it increasingly competes with countries that engage in distortionary practices such as non-transparent subsidies, "bounty" payments for the inclusion of specific technologies in standards, and government-coordinated bloc voting.[4] To this end, TIA supports the clarification of the R&D tax credit to include expenses related to standards development and the establishment of transparent, competitive grants for participation in standards development activities similar to such programs in the EU, Japan, and other global partners.

(C) information and cybersecurity practices and standards of the ICT sector with specific regard to the risks identified in paragraph (iv) above. The Department of Commerce and the Department of Homeland Security are specifically interested in comments related to validation standards of component and software integrity, standards and practices ensuring the availability and integrity of software delivery and maintenance, and security controls during the manufacturing phase of ICT hardware and components;

[4] U.S.-China Economic and Security Review Commission, *Section 2: The Chinal Model: Return of the Middle Kingdom* (available at https://www.uscc.gov/sites/default/files/2020-12/Chapter_1_Section_2--The_China_Model-Return_of_the_Middle_Kingdom.pdf).

TIA has long argued that the ICT industry is in the best position to implement best practices and standards aimed at mitigating vulnerabilities in the ICT supply chain. That is why we have worked with the ICT industry to create a Supply Chain Security Standard,[5] known as SCS 9001, that directly supports the policy objectives listed in the Supply Chain EO as they affect the U.S. ICT Supply Chain. SCS 9001 provides information and cybersecurity practices and standards to protect the ICT sector from risks that may disrupt or compromise supply chains. In addition, it will help identify if hardware and software come from entities that adhere to the rule of law, fall in line with global best practices as they pertain to transparency and disclosure, and comply with U.S. and international sanctions.

SCS 9001 is the ICT industry's first comprehensive and measurable standard designed to protect an organization's supply chain. Built upon ISO 9001 and a QMS foundation and focused on the ICT supply chain, it identifies key supply chain processes and defines standards for those processes, including how they will be evaluated and measured. SCS 9001 will also be third-party certified, leveraging an existing global network of accreditation bodies and certification bodies to enable organizations to implement, measure, and improve their supply chain processes.

Supply Chain Attacks Have Shown a Sharp Increase Since 2017

In 2019, TIA and its members foresaw the risks to supply chains and initiated an effort to create SCS 9001 to protect supply chains from compromised hardware and software, as well as nefarious entities. Supply chain attacks have shown a sharp increase starting in 2017.[6] These

[5] *See eg.* SCS 9001 Supply Chain Security Standard : Executive Summary, TIA, (available at https://bit.ly/SCS_ExecSummary); SCS 9001: ICT-Specific Standard for Global Supply Chain Security White Paper, April 2021, TIA, (available at https://tiaonline.org/what-we-do/technology-programs/supply-chain-security/scs-9001-ict-specific-standard-for-global-supply-chain-security/).

[6] Herr, Trey. Loomis, William. Scott, Stewart. Lee, June. *Breaking Trust: Shades of Crisis Across an Insecure Supply Chain*, Atlantic Council, Figure 1 (July 26, 2020) (available at

attacks are popular, impactful, and have been used to great effect by rogue bad actors and state actors alike.

Recent cyberattacks have increasingly utilized open source software as an attack vector. Initially, open source attacks focused on exploiting publicly disclosed software vulnerabilities that were left unpatched. The Apache Struts incident at Equifax is an example of this type of attack. However, recent attacks have grown more sophisticated, and attackers are now actively injecting malicious code into open source projects. The Octopus Scanner malware that targeted the NetBeans open source integrated development environment, is an example of this type of next generation supply chain attack, which have increased 430% since July 2019.[7]

These attacks have been able to exploit open source projects due to their open nature and because their wide adoption that allows bad actors to infect a large number of services and software. Some open source contributors indeed have others review their software before it is accepted. While large open source projects, such as Linux, have a very large pool of experienced reviewers, smaller projects may not.

The "event-stream" hack which targeted the Copay cryptocurrency wallet in 2018, is an example of a smaller project being attacked. In this instance, although only one developer maintained the Copay software, it was still a small open source project that had a big impact. This software is downloaded 1.5 million times a week and is used in 1,600 other open source

https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/).

[7] *2020 State of the Software Supply Chain,* Sonatype, Figure 1C (available at https://www.sonatype.com/hubfs/Corporate/Software%20Supply%20Chain/2020/SON_SSSC-Report-2020_final_aug11.pdf).

projects, that are also downloaded, thus exposing millions of users through a seemingly small breach.[8]

TIA's SCS 9001 Directly Supports the Supply Chain EO's Policy Objectives Listed as they Affect U.S ICT Supply Chains

Version 1.0 of SCS 9001 will be released before the end of 2021, and a draft version was released in early October 2021 for review purposes. The current version is over a hundred pages and at a high-level covers the requirements, controls, and measurements to increase ICT supply chain security. Requirements and controls cover processes related to organization, leadership, planning, support, and operations. Measurements are focused on performance evaluation and improvement. While the standard is extensive, these comments will focus on and include excerpts from a few specific areas that are most closely related to the policy objectives listed in the Supply Chain EO.

SCS 9001 Provides Information and Cybersecurity Practices and Standards to Protect the ICT Sector from Risks that may Disrupt or Compromise Supply Chains

SCS 9001 is a validation standard that will help ensure component and software integrity. It will help ensure the integrity of software delivery and maintenance, as well as provide security controls during the manufacturing phase of ICT hardware and components. The following are excerpts from the standard that we believe will provide useful examples of requirements and controls that address the security of software and hardware components:

Section 8.3.4.SC.3 identifies requirements for Test Verification and Validation processes. In addition to requiring the organization to have a test verification and validation process, it also requires the organization to perform that same process on third-party and open source software.

[8] Franklin, Chris. *How Hackers Infiltrate Open Source Projects*, Dark Reading (June 27, 2019) (available at https://www.darkreading.com/application-security/how-hackers-infiltrate-open-source-projects-/d/d-id/1335072).

> **Section 8.3.4.SC.3 – Test Verification & Validation Process**
> The organization shall:
> a) identify the security aspects during the verification and validation activities using various testing techniques such as security testing, privacy & data integrity testing and vulnerability testing,
> b) perform security verification and validation procedures and analyze security-focused results against any established expectations and success criteria,
> c) record verification and validation results and track to closure any security anomalies encountered, including those related to suppliers,
> d) maintain traceability of the verification and validation tests to the system requirements,
> e) obtain customer agreement that the system or system element meets the security requirements, and
> f) establish acceptance testing programs and related criteria for new information systems, upgrades, and new versions.
> **NOTE**: When using open source or any third-party content, it is the responsibility of the organization to perform necessary vulnerability assessments and/or tests to satisfy security requirements.

Section 8.3.5.SC.1 on Software Provenance requires organizations to maintain software identification and traceability, including creating a software Bill of Material ("SBOM").

> **8.3.5.SC.1 – Software Provenance**
> In order to assure software identification and traceability, the organization shall create a process that assists in the recording of system and component origin along with the history of, the changes to, and the recording of who made the changes.
> The organization shall define and implement methods into a software identification process that will assure the above and create a software Bill of Materials ("SBOM") for all software, firmware and supporting logic used in the creation of product or services elements.

This section goes on to provide more detailed requirements including:

- **Authenticity/Legitimacy** - Methods to establish that the software is from the claimed source, author, release number, location, license information, etc.
- **Integrity** - Methods to assure that a comprehensive risk analysis has been conducted of the software, any vulnerabilities requiring mitigation have been addressed, and to verify removing vulnerabilities that could be exploited.
- **Verifiability** - Methods that provide the ability for a user to evaluate the software assuring that the code has not been tampered with.
- **Legitimacy** - Methods to establish that the code was acquired from permitted and authorized sources, can only be modified by authorized means, and is used with licensed permission to operate within the approved government or business purpose.

SCS 9001 will Help Identify if Hardware and Software comes from Entities that Adhere to the "Rule Of Law"

Section 4 of the standard includes procedures requiring the organization to address statutory, regulatory, and contractual requirements.

> **Section 4.2.SC.1 – Relevant Legislative Statutory, Regulatory, Contractual Requirements**
> Appropriate procedures shall be implemented to address the following relevant requirements:
> a) contractual,
> b) legislative,
> c) statutory,
> d) regulatory,
> e) intellectual property rights, and
> f) use of proprietary software products.
> The organization's approach to meeting these requirements shall be explicitly identified and documented.

Section 4 also requires organizations to collect and report corporate principles of law that provide transparency of factors related to the rule of law.

> **4.2.SC.2 – Collect and Report Corporate Principles of Trust**
> Transparency on factors related to "Rule of Law" and business practices are important in evaluating the level of trust for an organization. Therefore, within the registration profile the organization shall:
> a) Provide the most recent country score for "Constraints on Government Powers" on the World Justice Project Rule of Law Index for the organization's domicile. (See https://worldjusticeproject.org/rule-of-law-index/factors/2020).
> b) Confirm that the company would not face countervailing duty determinations pegged using methodology for "non-market economies" absent a judgement from the World Trade Organization appellate body.
> c) Confirm that lines of officially supported export credit provided for the organization's product or service sales meet the Transparency Procedures of the Organization for Economic Co- operation and Development Arrangement on Officially Supported Export Credits.
> d) Identify whether the organization is public or private and if public, which global stock exchanges the organization is listed.
> e) Confirm that:
>
> 1) There are no legal requirements to select persons affiliated with any particular political party or government entity for the organization's Board of Directors.

2) There are no legal requirements to establish units of any political parties inside of a company.

f) Confirm that the organization’s Board of Directors include independent directors.

g) Confirm the company's financial statements are duly audited by an accredited external accounting firm.

h) To understand the organization’s ability to comply with international laws and standards pertaining to corrupt practice or bribery, the organization shall:

1) Provide a copy of their anti-corruption or anti-bribery policy, as well as any relevant certifications related to anti-corruption/anti-bribery compliance.

2) List any consent decrees, admissions of guilt, or any judgements rendered against the company by any government relating to corrupt practices or bribery in the past 10 years.

3) Identify judgement(s) from national authorities from any national authorities from the last 10 years pursuant to violations of United Nations Security Council Resolution 2231 which imposed sanctions on Iran.

4) Identify any judgement(s) from any national authorities from the last 10 years pursuant to the terms of United Nations Security Council Resolutions 1718, 1874, 2087, 2094, 2270, 2321, 2371, 2375, or 2379 imposing sanctions on North Korea.

SCS 9001 will Help Identify if Hardware and Software come from Entities that Support U.S. Security Controls and Sanctions

Section 8.3.5.SC.1 of SCS 9001 deals with software provenance and requires methods that will support organizational compliance with U.S. national security controls. It will do so by helping organizations identify whether code was acquired from authorized sources and providing attributes related to its provenance including author, build location (i.e., country), and relevant export restrictions. While the standard does not require a verification against the FCC’s Covered Entity List, the Department of Commerce’s Bureau of Industry and Security Entity List, or other government security lists such as the Treasury Department’s Specially Designated Nationals and Blocked Persons List, it does require information that would enable U.S. organizations to do so and ensure they are adhering to U.S. law. In fact, it would allow organizations from any country to do the same with regard to their own country’s laws or those of the United States.

> **Legitimacy** - Methods to establish that the code was acquired from permitted and authorized sources, can only be modified by authorized means, and is used with licensed permission to operate within the approved government or business purpose.
> Provenance - Methods so that users can make trust determinations to determine the software source (origination) and other attributes that can provide information related to its legitimacy, such as:
> 1) owner,
> 2) author,
> 3) release (version) number,
> 4) build location – country and/or other appropriate controls
> 5) license information, restrictions etc., such as:
>   i. cloud environment
>   ii. country where it executes
>   iii. export restrictions
> 6) versions change history considerations

Section 8 also requires an SBOM which includes a requirement to identify supplier name, open source and third-party content, and whether the software is included in or derived from other software.

> Creation of SBOM for the product. The organization shall create a SBOM that conforms with the requirement of this standard for each software or firmware deliverable. The SBOM should include:
> 1) baseline component information:
>   i) mapping to existing formats
>   ii) supplier name
>   iii) component name or unique identifier
>   v) version
>   vi) component hash, or equivalent
> 2) compatibility requirements
> 3) mapping to existing formats
> 4) relationship (included in or derived from)
> 5) component relationships
> 6) open source software content free and open source content, and third party content

We hope this brief look into TIA's comprehensive SCS9001 standard provides a useful example of how the ICT industry is in the best position to create standards and best practices aimed at creating a more resilient ICT supply chain.

(E) location of key design, manufacturing, software development, integration, and production assets, with any significant risks identified in paragraph (iv) above posed by the asset's physical location or the distribution of these facilities;

The supply chain for the ICT sector is deeply global with manufacturing operations that span the world from the companies that design the products, to contract manufacturers that often build the products, to dense networks of suppliers and subcontractors. Just to pull out one component – semiconductors can require more than 1,000 discrete steps in the manufacturing process and pass through borders more than 70 times before the chip meets the consumer.[9] Access to these global supply chains can support reliability through a diverse ecosystem of redundant suppliers and drives down costs to connect consumers who rely on access to high-quality, affordable broadband. They are also essential to the continued competitiveness of trusted ICT providers who compete around the world with state-affiliated firms supported by massive government subsidies.[10] These supply chains power American jobs and American exports. For instance, in 2019 the United States exported $35.9 billion in telecommunications equipment.[11]

Ongoing consideration by the Department of Defense, General Services Administration, and National Aeronautics and Space Administration of changes to "Buy American" provisions of the Federal Acquisition Regulations ("FAR") have the potential to undermine the U.S. ICT manufacturing supply chain. Specifically, the consideration of measures extending the scope of "Buy American" provisions of the FAR to include commercial IT products could:

[9] Khan, Saif M., Mann, Alexander, Peterson, Dahlia, *The Semiconductor Supply Chain: Assessing National Competitiveness,* Center for Security and Emerging Technology (January, 2021), (available at https://cset.georgetown.edu/publication/the-semiconductor-supply-chain/).

[10] Yap, Chuin-Wei, *State Support Helped Fuel Huawei's Global Rise*, The Wall Street Journal (Dec. 25, 2019) (available at https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736).

[11] Tech Trade Snapshot 2020, CompTIA, (May, 2020) (available at https://connect.comptia.org/content/research/tech-trade-snapshot-2020).

1) Undermine the ability of the federal government and other public sector entities to access up-to-date information technology solutions.
2) Cause other governments to restrict the sale of U.S. ICT products to public sector users.
3) Balkanize supply chains by dividing production lines into the private sector and public sector lines thereby leasing to substantial cost increases, issues with systems integration and backwards compatibility, and potential quality problems in public sector products.

Some companies have noted that given the investment of time and money that this would take, eliminating the IT exemption would force them to reassess their U.S. public sector business. This is germane to this filing given that the Proposed Rule on Amendments to the FAR Buy American Act Requirements refers to the Supply Chain EO and the quadrennial critical supply chain review as the basis for an enhanced price preference.[12]

Similarly, ongoing efforts to include Buy American provisions in the Bipartisan Infrastructure Framework (BIF) could limit – or potentially halt entirely – efforts to expand broadband access. There is no combination of vendors that could build out all elements of a greenfield wireless network using exclusively U.S.-origin components, and waivers to those requirements will be necessary if the government wants to make meaningful investments in broadband.

(H) relevant workforce skills, best practices, and identified gaps in the availability and/or adequacy of domestic education and training resources necessary to fulfill future workforce needs;

The U.S. faces a shortfall of skilled workers needed to deploy broadband across the country, to win the race to 5G, and to ensure robust fiber, mobile, and fixed wireless networks. Needed investments in broadband infrastructure will increase demand on a labor force already in

[12] Federal Acquisition Regulation: Amendments to American Act Requirements, Proposed Rule, Department of Defense, General Services Administration, National Aeronautics and Space Administration (Jul. 7 2021) (available at https://www.federalregister.gov/documents/2021/07/30/2021-15881/federal-acquisition-regulation-amendments-to-the-far-buy-american-act-requirements).

short supply. To improve the efficiency of federal funding, a corresponding initiative is needed to develop a workforce properly trained with the skills to deploy next generation wired and wireless networks.

5G alone is projected to create three million direct and indirect jobs by 2025 and contribute $500 billion annually to the U.S. economy.[13] Current 5G design and buildout has already created over 106,000 direct jobs in installation and engineering.[14] Overall, the U.S. telecommunications industry employs 672,000 workers, with average annual wages that exceed $77,500.[15] At the current rate of deployment, there will be 850,000 more new direct broadband and 5G jobs through 2025, which federal support would accelerate. [16] While the jobs are there, the above snapshot shows that our American workforce is not currently ready to fill them. Some solutions to this workforce challenge include:

- Support employers to expand registered apprenticeships and associated technical instruction and certification costs,
- Bolster the capabilities of institutions of higher education and other institutions to ensure a diverse workforce capable of deploying fiber and 5G infrastructure for commercial mobile and fixed wireless networks,
- Expand public-private partnerships with community colleges, universities, and other institutions to develop degrees and programs of study on broadband deployment and 5G training, and
- Streamline immigration procedures for H1B and other high-skilled worker programs to ensure that innovative U.S. ICT companies can leverage a global talent pool.

(viii) prioritization of the “critical goods and materials” and “other essential goods and materials,” including digital products, identified in paragraphs (i) and (ii) above for the purpose of identifying options and policy recommendations. The prioritization shall be based on statutory or regulatory requirements; importance to national security, emergency preparedness, and the policy set forth in section 1 of E.O. 14017;

[13] Coalition Letter on Workforce Issues, *US Telecom* (January 27, 2021) (available at https://www.ustelecom.org/wp-content/uploads/2021/01/workforce-letter-jan-2021_senate.pdf).
[14] Id.
[15] Id.
[16] Id.

TIA has a long history of supporting technology-neutral policies to expand connectivity and enhance American innovation. We believe that government policies that utilize all available technologies to address problems, such as closing the digital divide, are more effective and flexible than policies that prioritize certain technologies at the expense of others. Prioritizing one method of connectivity (e.g. fiber, wireless, WiFi, or satellite) or type of end user interface (e.g. laptops, phones, IoT devices, connected vehicles, etc.) runs the risk of picking winners and losers among the ICT industry, and forcing solutions where they might not be the most cost effective or efficient choice due to rigid policy. Policies that prioritize or mandate one technology over another also raise the risk of potentially directing government funds and attention toward a solution that does not meet consumer needs or becomes irrelevant with the pace of technological development. To that end, we urge BIS and the Administration to remain flexible in the solutions they recommend for increasing the resiliency of the U.S. ICT supply chain and resist the urge to mandate or prioritize one ICT technology over another.

(ix) specific policy recommendations important for ensuring a resilient supply chain for the ICT industrial base. Such recommendations may include, but are not limited to, sustainably reshoring supply chains and developing or strengthening domestic design, components, and supplies; cooperating with allies and partners to identify alternative supply chains; building redundancy into domestic supply chains; ensuring and enlarging stockpiles; developing workforce capabilities; enhancing access to financing; expanding research and development to broaden supply chains; addressing risks due to vulnerabilities in digital products relied on by supply chains; addressing risks posed by climate change; strengthening supply chain security; and any other recommendations;

As the Department of Commerce and BIS examines the risks to the ICT supply chain, it is important that they do not set aside quality work product focused on ICT policy recommendations that have been collected through past government-industry consultations. For instance, last summer the Department of Commerce issued a Request for Comment on an overarching U.S. government plan to implement 5G, as required by the Secure 5G and Beyond

Act.[17] The ICT industry then provided extensive feedback to this request for comment with substantial policy recommendations that government could adopt to streamline U.S. 5G deployment.[18] The National Telecommunications Industry Administration then released a plan that included a number of policy recommendations salient to the questions raised by the Bureau of Industry and Security in this docket, though the report has languished its release. [19]

TIA urges BIS and the Department of Commerce, on the whole, to not let this extensive consultation with industry on the nation's next-generation ICT networks go to waste, and we recommend revisiting this extensive docket and report pursuant to the National Strategy to Secure 5G Implementation Plan.

CONCLUSION

TIA appreciates the opportunity to provide comments to BIS on risks in the ICT supply chain. We stand ready to work with the Bureau and other U.S. government stakeholders to ensure that the ICT supply chain is secure and ready to weather future shocks.

/s/ Tom McGarry
Vice President, Standards

[17] Request for Comments on the National Strategy to Secure 5G Implementation Plan, National Telecommunications and Information Administration, Department of Commerce, Docket No. 200521-0144 (May 28, 2020) (available at https://www.federalregister.gov/documents/2020/05/28/2020-11398/the-national-strategy-to-secure-5g-implementation-plan).

[18] Comments on the National Strategy to Secure 5G Implementation Plan, *National Telecommunications and Information Administration*, (June 29, 2020) (available at https://www.ntia.gov/federal-register-notice/2020/comments-national-strategy-secure-5g-implementation-plan).

[19] National Strategy to Secure 5G Implementation Plan, *National Telecommunications and Information Administration*, (January 6, 2021) (available at https://www.ntia.gov/federal-register-notice/2020/comments-national-strategy-secure-5g-implementation-plan).

Colin Black Andrews
Senior Director, Government Affairs

Patrick Lozada
Director, Global Policy

TELECOMMUNICATIONS INDUSTRY
ASSOCIATION
1310 N. Courthouse Road
Suite 890
Arlington, VA 22201
(703) 907-7700

Filed: November 4, 2021