Before the
**NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION**
**U.S. DEPARTMENT OF COMMERCE**
Washington, DC 20230

| | | |
|---|---|---|
| In the Matter of | | |
| | ) | |
| The National Strategy to Secure 5G | ) | Docket No. 200521-0144 |
| Implementation Plan | ) | RIN-0660-XC047 |

# COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION


Colin Black Andrews
Director, Government Affairs

Patrick Lozada
Director, Global Policy

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


Filed: June 25, 2020

## TABLE OF CONTENTS

Before the
**NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION**
**U.S. DEPARTMENT OF COMMERCE**
Washington, DC 20230

| | | |
|---|---|---|
| In the Matter of | | |
| | ) | |
| The National Strategy to Secure 5G | ) | Docket No. 200521-0144 |
| Implementation Plan | ) | RIN-0660-XC047 |

**COMMENTS OF THE**
**TELECOMMUNICATIONS INDUSTRY ASSOCIATION**

The Telecommunications Industry Association (TIA) appreciates the opportunity to provide input from industry regarding the National Strategy to Secure 5G Implementation Plan.[1] As both an advocacy organization and a standards-setting body, TIA represents hundreds of global manufacturers and vendors of information and communications technology ("ICT") equipment and services that are supplied to the owners and operators of communications networks, enabling operations across all segments of the economy. Our member companies design, produce, and sell equipment and services in countries around the world that leverage modern global supply chains, and each company has a vital stake in mitigating the risks present in the ICT supply chain and encouraging participation in international ICT standards designating organizations. As such, we welcome the opportunity to discuss the broad range of important questions raised by the RFC designed to facilitate a stronger deployment of critical 5G technologies.

[1] National Telecommunications and Information Administration, *The National Strategy to Secure 5G Implementation Plan*, Notice, Request for Public Comments, 85 FR 32016, Docket No. 200521–0144 (May 28, 2020) ("RFC").

## I. The Implementation Plan for the National Strategy to Secure 5G Should Empower Industry-Driven Efforts to Secure the ICT Supply Chain.

***Line of Effort Two:*** *Assess Risks to and Identify Core Security Principles of 5G Infrastructure.*

*WHAT FACTORS SHOULD THE U.S. GOVERNMENT CONSIDER WHEN EVALUATING THE TRUSTWORTHINESS OR POTENTIAL SECURITY GAPS IN U.S. 5G INFRASTRUCTURE, INCLUDING THE 5G INFRASTRUCTURE SUPPLY CHAIN? WHAT ARE THE GAPS?*

### a. The U.S. needs a whole-of-government approach that adds transparency to the ICT supply chain.

One of the U.S. government's top priorities when evaluating security gaps in 5G infrastructure should be ensuring transparency in the ICT supply chain. Over the past decade, the fragmentation of the ICT supply chain has resulted in a growing number of suppliers, manufacturers, and service providers developing and deploying the hardware and software that comprise the world's telecommunications infrastructure. This shift has enabled the globalization of ICT resources and is driving networks to become more software-driven and reliant on white-box equipment and open interfaces that gives users more choices and flexibility. With this new network landscape, the ICT supply chain has become increasingly complex and vulnerable at any point along its lifecycle. With more equipment, connected devices, and global players than ever, security risks are at an all-time high. These risks include data breaches, denial-of-service attacks (DDOS), concerns with counterfeit components, or components that come from a compromised vendor or a source that poses a threat to national security.

To mitigate these risks, the U.S. government must address security concerns with a comprehensive, whole-of-government approach to ensure consistency among the numerous government and public-private initiatives focused on supply chain security that are currently underway. Individual actions cannot succeed in securing the supply chain if they operate in a vacuum that ignores the existing ecosystem of mutually interrelated government activities. These

include ongoing rulemaking procedures before various agencies, requirements from executive orders, as well as pending and existing legislation in Congress. TIA appreciates the Administration's willingness to receive industry input on these efforts and has been an active participant in those dockets, but the broad nature of the questions posed by the RFC underscores the likelihood of continuing government action focused on supply chain security.[2] In drafting the Implementation Plan, the Administration has a unique opportunity to ensure coordination with the various efforts of the interagency and ensure that these efforts function harmoniously.

While government action to help mitigate the vulnerabilities of the ICT supply chain is important, any fruitful whole-of-government approach to supply chain security must empower the numerous efforts led by industry focusing on this topic. TIA appreciates the Administration's willingness to work with industry stakeholders through public-private ventures such as the Department of Homeland Security's ICT Supply Chain Risk Management Task Force and the Information Technology and Communications Sector Coordinating Councils. However, these public-private partnerships are not the only initiatives focusing on adding transparency and security to the ICT supply chain. The U.S. government should support industry-led efforts as well as leverage existing government and private sector partnerships to facilitate an effective dialog for supply chain security policy.

---

[2] Comments of the Telecommunications Industry Association, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89 (filed Feb. 3, 2020), *available at* https://ecfsapi.fcc.gov/file/10203229746606/TIA%20Final%20USF%20Comments.pdf; Comments of the Telecommunications Industry Association, *Securing the Information and Communications Technology and Services Supply Chain*, Dkt. No. 191119-0084, RIN-0605-AA51 (Jan. 10, 2020), *available at* https://mk0tiamultisitee8xgk.kinstacdn.com/wp-content/uploads/2020/01/TIA-Final-Comments-on-Commerce-Supply-Chain-Rules.pdf

The vast number of initiatives led by the government and industry focusing on supply chain security presents a challenging landscape to track and harmonize. To that end, TIA supports the Cyberspace Solarium Commission's recommendation for a National Cyber Director as a coordination point for the various efforts currently underway across the U.S. government.[3] In its report released in March, the Solarium Commission recommended the establishment of a senior official as a National Cyber Director as well as creating an accompanying office at the White House. TIA supports this effort of establishing a top-of-line government official to coordinate the U.S. government's efforts on cybersecurity and would recommend that this position also oversee ongoing supply chain security efforts.[4]

*WHAT CONSTITUTES A USEFUL AND VERIFIABLE SECURITY CONTROL REGIME? WHAT ROLE SHOULD SECURITY REQUIREMENTS PLAY, AND WHAT MECHANISMS CAN BE USED TO ENSURE THESE SECURITY REQUIREMENTS ARE ADOPTED?*

**b. Addressing the risks present in the ICT industry supply chain requires an industry-led certification scheme that is both global and flexible.**

As a foundational matter, any effective security mechanism for the ICT supply chain requires a level of verification and accountability that can be measured and certified only by individual companies with an intricate understanding of their supply chains. TIA believes that the most effective mechanisms for certifying ICT supply chain risk management can only come from the creation of industry-driven consensus-based standards, measurements, and benchmarking that form a consistent, common, and widely accepted set of industry requirements. Additionally, an industry-driven standard helps ensure that requirements are implemented in

[3] U.S. CYBERSPACE SOLARIUM COMM'N REP. (2020), https://www.solarium.gov/report

[4] While TIA supports the creation of a National Cyber Director position, TIA does not support the idea that the NCD should "align opinions" of private-sector U.S. entities participating in global standards development as articulated in Section 2.1.2 of the Solarium Commission Report. TIA finds this proposal both unnecessary in light of the important coordinating role played by NIST, and undesirable to the extent that it risks damaging the private sector led model of standards development that has driven innovation in ICT.

robust and timely manner, which accelerates adoption, and keep the requirements focused on the most critical aspects of securing the ICT supply chain rather than edge case requirements, facilitating a more cost-effective implementation. Any industry-driven standard, however, should still provide ample opportunities for government involvement and support for its adoption.

Any standard or certification program focusing on supply chain security not only needs to be industry-driven, but it also needs to include global requirements and must constantly adapt as new threats are discovered. The ICT market is global, and governments can develop greater confidence in ICT supply chains by facilitating a common set of standards and certifications in order to allow manufacturers to sell their IoT products in all major markets around the world. The global nature of the ICT community also underscores the necessity for a certification system that responds and adapts to emerging threats. TIA believes the best way to ensure this adaptability is by creating a program that can respond to live-data submitted by industry utilizing it in order to promote information sharing regarding emerging threats or vulnerabilities in their supply chains.

*ARE THERE STAKEHOLDER-DRIVEN APPROACHES THAT THE U.S. GOVERNMENT SHOULD CONSIDER TO PROMOTE ADOPTION OF POLICIES, REQUIREMENTS, GUIDELINES, AND PROCUREMENT STRATEGIES NECESSARY TO ESTABLISH SECURE, EFFECTIVE, AND RELIABLE 5G INFRASTRUCTURE?*

**c. TIA would welcome the government's support for its efforts to build a measurable and verifiable standard on supply chain security.**

TIA is currently building a global standard and benchmarking tool that measures the risks present in each vendor's supply chain in real-time, with the goal of having pilot third party certifications begin in mid-2021. QuEST Forum, which merged with TIA in 2017, is in the process of developing a comprehensive approach to improving supply chain security by incorporating proven elements of existing industry-driven standards and adding new ICT

requirements that address modern networks and their supporting technologies. This standard would function as a standalone addendum to the TL-9000 Quality Management System, which is run by QuEST. TL-9000 is based on ISO-9001 but is specifically designed for use by the telecommunications industry. TL-9000 has been leading the supply chain quality requirements for the ICT industry for over 20 years.

TIA believes that security is a vital element of quality, which is why this new standard would be built upon the existing TL-9000 quality management system database. This addendum to TL-9000 will make use of our anonymous benchmarking engine to collect data securely from registered companies and then produce anonymous industry results that can be used by organizations to benchmark their performance and implement appropriate improvement initiatives. Using this benchmarking engine with continuous membership feedback will bring in beneficial practices of customer involvement in refining requirements, structured life cycle management, and use of measurement to drive continual improvement.

Over the past year, TIA has been active in working with ICT industry members and U.S. government stakeholders on building this supply chain security-focused addendum that would:

i. Define a set of security requirements through comprehensive third-party assessments, measurement, and benchmarking.
ii. Provide transparent, comprehensive reporting that identifies trusted ICT manufacturers, buyers, suppliers, service providers, integrators, and contractors through third-party certification processes.

iii. Eliminate existing gaps by developing new comprehensive industry-driven standards to ensure the security of devices, equipment, and networks that comprise the ICT supply chain.

iv. Build upon existing work done by other standards and government documents, such as NIST 800-161 and the Cybersecurity Maturity Model Certification (CMMC), but utilizing only the subset of requirements that apply to the broader ICT supply chain.

TIA strongly believes that this program can solve many of the concerns held by industry and the U.S. government when it comes to exposing risks and vulnerabilities present in the ICT supply chain. TIA would welcome the opportunity to continue working with U.S. government stakeholders to ensure agencies' supply chain risk mitigation concerns are adequately met by our final standard and third-party certification regime.

## II. The Implementation Plan should support policies that create favorable trading conditions for suppliers of trusted telecommunications equipment, and that incentivize U.S. participation in international standard setting bodies.

***Line of Effort Four:*** *Promote Responsible Global Development and Deployment of 5G.*

*HOW CAN THE U.S. GOVERNMENT BEST LEAD THE RESPONSIBLE INTERNATIONAL DEVELOPMENT AND DEPLOYMENT OF 5G TECHNOLOGY AND PROMOTE THE AVAILABILITY OF SECURE AND RELIABLE EQUIPMENT AND SERVICES IN THE MARKET?*

### a. The U.S. government should continue to support the use of international standards.

International standards have long been the bedrock of the ICT sector because of the inherent need for interoperability in the context of global communications. While international standards are desirable in nearly all sectors, they are fundamental to ICT products because without them the basic function of the products is diminished. While certain international

standards bodies have flaws, these criticisms need not dissuade the U.S. from engaging and participating. Rather, it is a call for the U.S. to deepen its engagement in international standards and strengthen its commitment to adopting and promoting international standards around the world.

Supporting and promoting the use of international standards is vital to U.S. ICT companies because these standards lower barriers to trade around the world, allowing trusted manufacturers of ICT equipment to develop products that are maximally interoperable and that can be manufactured and designed at scale. By using 3GPP's standards for 5G radio access equipment, for example, companies can sell roughly the same components and network gear to companies in the United States that they do in Europe, Africa, or Central Asia. This worldwide compatibility decreases prices, and allows companies to focus on quality, safety, and innovation. International standards are created under frameworks that require transparent processes that promote the development of more secure technologies.

**b. Country-specific standards for ICT equipment create costs and raise security challenges.**

The flip side of promoting the use of international standards is vigorously opposing the use of country-specific standards for ICT equipment. In addition to imposing costs on trusted manufacturers of ICT equipment by forcing them to re-engineer products for specific markets, country-specific ICT standards also boost equipment from untrusted sources. Unable to compete with the existing framework in terms of security, innovation, and prices, these firms compete by leveraging access to regulators or non-transparent domestic standards-setting bodies.

Country-specific ICT standards are not limited to strategic competitors of the United States. India, a U.S. ally, is promoting a 5G New Radio specification that uses a modulation

technique known as as π/2 BPSK to address the Low-Mobility-Large-Cell (LMLC) scenarios for rural India. India had previously promoted this technology in the context of 3GPP but was unsuccessful in gaining sufficient support in 3GPP to make it a mandatory feature. They have thus decided to engage in "forum-shopping" behaviour by taking their proposal to the ITU, where they expect to face less scrutiny. These specifications contain modifications on top of the 3GPP spec with no meaningful technical advantages, while generating incompatibilities with existing 3GPP specifications. While this proposal was submitted by India's TSDSI in the context of an international standards development organization, it is being pursued first and foremost as a domestic standard in a way that will lead to a costly, isolated, and less secure ecosystem. Where such exclusionary, country-specific standards exist or are proposed, TIA believes it should be the policy of the U.S. government to oppose them.

**c. The U.S. government should support engagement by both U.S. companies and global partners in standards setting organizations.**

The United States should support engagement in relevant standards development organizations by both U.S. entities and from non-U.S. trusted vendors. Additionally, the U.S. should work to ensure that the processes these organizations use remain open, transparent, and fair.

*HOW CAN THE U.S. GOVERNMENT BEST ENCOURAGE AND SUPPORT U.S. PRIVATE SECTOR PARTICIPATION IN STANDARDS DEVELOPMENT FOR 5G TECHNOLOGIES?*

**d. Re-affirm and strengthen the public-private partnerships that put market-driven innovation in the driver's seat.**

America's market-driven, private sector-led approach to global standardization is different from the model practiced by many other countries and regions. This difference, however, is a source of strength. U.S. firms are global leaders across a range of ICT fields, and

while U.S. firms do not dominate 3GPP's 5G standards development, the best way to facilitate U.S. leadership in this space is to bolster private-sector innovation. In this context, the U.S. plays an important role as a consultative partner and facilitator but should not – as the Cyberspace Solarium Commission has recommended – coordinate U.S. contributions with the aim of "unified promotion of the most technically secure standards."[5] Top-down coordination like this belies existing mechanisms to facilitate dialogue between policymakers and companies engaged in standards development forums, and if not approached carefully could prioritize bureaucracy and collusion over technical merit and market-driven innovation.

**e. U.S. participation in standards development should not be limited by Export Administration Regulations.**

The assertion by the Commerce Department's Bureau of Industry and Security (BIS), in a series of filing pursuant to the addition of Huawei to the entity list, that standards development falls under the scope of Export Administration Regulations (EAR) has introduced significant uncertainty regarding the ability of U.S. firms to fully participate in international standards development.[6] As a direct result of this action, U.S. companies have been forced to pare back engagement at international standards development organizations both in the context of formal proposals and information-sharing, and in the day-to-day, open communication that takes place

[5] *Supra* note 3 at 3.

[6] U.S. Dep't of Com., Bureau of Indus. & Sec., General Advisory Opinion Concerning Prohibited Activities in the Standards Setting or Development Context When a Listed Entity Is Involved (2020), *Additions to the Entity List*, 84 FR 22961 (May 21, 2019); *Temporary General License*, 84 FR 23468 (May 22, 2019) (effective May 20, 2019 through August 19, 2019), https://www.bis.doc.gov/index.php/documents/advisory-opinions/2437-general-advisory-opinion-concerning-prohibited-activities-in-the-standards-setting-or-development-context-when-a-listed-entity-is-involved/file; U.S. Dep't of Com., Bureau of Indus. & Sec., *Temporary General License*, Final Rule, 84 FR 43487, Docket No. 190814-0012, (Aug. 21, 2019) (effective Aug. 21, 2019 through Nov. 18, 2019), https://www.federalregister.gov/documents/2019/08/21/2019-17920/temporary-general-license-extension-of-validity-clarifications-to-authorized-transactions-and; U.S. Dep't of Com., Bureau of Indus. & Sec., *Temporary General License*, Final Rule, 84 FR 23468, Docket No. 90513445–9459–02, (May 22, 2019) (effective May 20, 2019 through August 19, 2019), https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2019/2397-84-fr-23468-temporary-general-license-rule/file

on the margins of standards development meetings. The result has been a blow to U.S leadership in standards-setting, with some U.S. working group chairs in 5G-related standards development organizations ceasing participation for fear that they might inadvertently violate export controls laws. Uncertainty around U.S. law in this area has even contributed to the decision by some SDOs – such as the RISC-V Foundation – to relocate from the United States to overseas.

While the recent modifications to the EAR allowing for broader participation by U.S. entities in the context of standards development activities through the creation of a specific exemption for Huawei is a step in the right direction, this narrow modification has not solved the broader problem.[7] Engineers from other companies identified on the BIS entity list also participate in international standards development activities, and restrictions on the ability of U.S. entities to participate in and lead standards-setting where these companies participate remain. More broadly though, the uncertainty around future additions to the entity list and subsequent restrictions on standards development pursuant to the EAR mean that U.S. entities will remain second-class citizens in these organizations until the U.S. government removes these restrictions on U.S. company participation.

From a legal perspective, clarifying that the EAR does not apply to standards development is consistent with the law itself and past application of similar coercive economic actions. 15 C.F.R. § 734.3(b) states that the following are explicitly not subject to the EAR:

[7] U.S. Dep't of Com., Bureau of Indus. and Sec., *Release of "Technology" to Certain Entities on the Entity List in the Context of Standards Organizations*, Interim Final Rule, Request for Public Comments, 85 FR 36719, Docket No. 200611-0158, (June 18, 2020), https://www.federalregister.gov/documents/2020/06/18/2020-13093/release-of-technology-to-certain-entities-on-the-entity-list-in-the-context-of-standards

4) Information and "software" that:

(i) Are published, as described in § 734.7;

(ii) Arise during, or result from, fundamental research, as described in § 734.8;

(iii) Are released by instruction in a catalog course or associated teaching laboratory of an academic institution;

(iv) Appear in patents or open (published) patent applications available from or at any patent office, unless covered by an invention secrecy order, or are otherwise patent information as described in § 734.10;

(v) Are non-proprietary system descriptions; or (vi) Are telemetry data as defined in Note 2 to Category 9, Product Group E

§ 734.7 of the EAR clarifies that unclassified "technology" or "software" is "published," and is thus not subject to the EAR when it has been made available to the public. In light of these provisions, TIA believes that discussions with representatives of listed entities in the context of legitimate standards-setting activities should not be subject to the EAR under existing statute. Similarly, the American National Standards Institute (ANSI) has noted that other economic sanctions such as the Treasury Department's Office of Foreign Assets Control (OFAC) application of sanctions pursuant to the SDN list specifically did not apply restrictions to participation in standards development activities because such interactions were public and intended to result in published standards.[8]

[8] Letter from Joe Bhatia, President and CEO of ANSI, U.S. Dep't of Com., Bureau of Indus. & Sec., Temporary General License, Final Rule, 84 FR 23468, Docket No. 90513445–9459–02 (June 6, 2019), https://share.ansi.org/shared%20documents/Standards%20Activities/Critical%20Issues/OFAC/ANSI-Letter-to-BIS.pdf

**f. The U.S. government should reinforce consistent U.S. government participation in relevant standards forums.**

To support the leadership of the U.S. private sector in standards development, the U.S. government should shore up its own presence at relevant international standards forums. To do this, policymakers should consider establishing multi-year funding lines and streamline processes with the goal of supporting sustained participation by designated staff. By expanding the U.S. government presence at relevant international forums, the U.S. government can help address the issue of certain non-market economies sending large, well-funded delegations to support their own favored industries.

In addition, the U.S. should not shrink away from participating in regional forums including the Asia-Pacific Economic Cooperation (APEC), the World Trade Organization (WTO), and various agencies and working groups within the United Nations. These forums present unique opportunities to advance and promote standards-setting best practices. Strong U.S. participation would reinforce the country's leadership while advancing its own 5G interests.

**g. The U.S. should be the best, most welcoming place to develop standards.**

The U.S. government should work towards making the U.S. the best, most welcoming place to develop standards and coordinate international standards development projects. This has direct benefits to the ability of American companies to participate in and lead standards by:

- decreasing travel, lodging, and incidental costs associated with attending internationals standards development meetings abroad;
- lowering perceived barriers to entry for U.S. small and medium enterprises; and
- giving American participants a "home-field advantage" where they can operate in their native time zone and language.

On the other end, non-U.S. companies or companies without any U.S. presence then face inverse monetary, time, and attention costs for standards events held in the United States, giving American companies and participants a comparative advantage.

The U.S. government can establish itself as the premier global standardization location by removing any unnecessary and burdensome restrictions on the ability of engineers to travel and participate in standards development activities. TIA staff have reported that it is increasingly difficult for foreign nationals to secure visas to travel to the United States in order to participate in standards development activities. Making it more difficult to obtain visas to the U.S. both weakens standards development programs by U.S. ANSI-accredited standards development organizations like TIA and makes it less likely that those standards are adopted internationally. To ameliorate this issue, the State Department should consider setting up lines of communication with U.S. standards development organizations to resolve issues in a timely fashion as they arise.

As a related point, retaining world-class engineering talent requires access to the world's best engineers. The recent decision by the Administration to suspend new visas for high-skilled foreign national granted under the H-1B visa program will further limit the pool of top standards development talent. Meanwhile, China's Ministry of Science and Technology has released a "High-End Foreign Experts Recruitment Plan" to bolster the country's expertise in key sectors such as telecommunications.[9] The U.S. government should consider lifting this suspension and expanding access to visas for high-skilled workers.

---

[9] Guanyu Shenbao 2020 NianDu Guojia Waiguo Zhuanjia Xiangmu De Tongzhi (关于申报 2020 年度国家外国专家项目的通知) [Notice on Applying for 2020 National Foreign Expert Projects], Keji Bu (科技部) [Ministry of Sci. & Tech.] (Jan. 10, 2020) translated by Ben Murphy, available at https://cset.georgetown.edu/wpcontent/uploads/t0100_belt_road_young_experts_EN-1.pdf, original Chinese

**h. The U.S. government should support voluntary standards generated by U.S. SDOs.**

U.S. standards reflect the traditional strengths of the American system in that they are consensus-based, transparent, and driven by the private sector. Given the U.S. government interest in promoting these values and U.S.-participation in international standards more generally, the U.S. government should consider finding ways to support these standards internationally. Supporting these standards abroad also reduces barriers to trade facing U.S. companies through increased interoperability, aligning the technologies used abroad with those used at home.

One example of how the U.S. can help do this is by ensuring compliance by America's trading partners with intellectual property rights associated with standards developed by U.S.-based SDOs as defined by OMB Circular A-119.[10] SDOs count on revenue from the sale of access to standards documents as a way to support cost recovery for standards development activities, however in many international contexts these documents end up being circulated without payment or authorization. This leads both to financial shortfalls, but also safety risks stemming from out-of-date or modified documentation. TIA recommends that the International Trade Administration and the Office of the U.S. Trade Representative work to support American standards by promoting their use where appropriate overseas and ensuring proper payment for engagement with these standards.

available at https://bs.nankai.edu.cn/_upload/article/files/50/76/1ccb741b40bc9c8de51bd61dab83/c47f1393-0250-47ac-a458-e8d230491830.docx

[10] OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB CIRCULAR NO. A-199 REVISED, MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES (1998). https://www.whitehouse.gov/wp-content/uploads/2017/11/Circular-119-1.pdf

*ARE THERE MARKET OR OTHER INCENTIVES THE U.S. GOVERNMENT SHOULD PROMOTE OR FOSTER TO ENCOURAGE INTERNATIONAL COOPERATION AROUND SECURE AND TRUSTED 5G INFRASTRUCTURE DEPLOYMENT?*

**i. Tax credits and incentives related to standards development would support U.S. standards leadership.**

In most cases, the development of standards is a relatively low-margin activity with profits that are only realized after multiple years of investment and effort. As a result, companies often lack sufficient internal incentives to make standards development a top priority and instead focus time and engineering talent in other areas. To make up for this gap and to counter countries like China that provide generous incentives to companies and engineers who are able to successfully have their proposals incorporated into global standards, TIA recommends that the United States government consider expanding R&D tax credits to encourage investments in standards development. These expanded tax credits should be scoped in broad terms to accurately account for the nature of investments companies make during the standards development process. Covered costs should include but not be limited to costs associated with travel and lodging need for purposes international standards development activities, costs associated with membership in standards development organizations, and incidental expenses.

**j. The U.S. should re-state its support of and commitment to the WTO Government Procurement Agreement.**

In order to promote international cooperation around secure and trusted 5G infrastructure, the U.S. government should continue to support the WTO Government Procurement Agreement (GPA). Because purchasers of networking equipment are state-owned telecommunications companies in many countries, the WTO GPA provides a vital mechanism to ensure transparency, accountability, and predictability in the global ICT market. Under the GPA, member countries must collect and publish statistics on their government procurement activities including the number and estimated value of contracts awarded and the country of origin of products and

services purchased. This knowledge can help stakeholders identify vulnerabilities in the global ICT supply chain and make informed decisions with respect to 5G infrastructure.

If the U.S. withdraws from the GPA – as some have suggested – it will weaken the ability of U.S. partners who rely on the GPA to supply trusted communications equipment to other GPA signatories. Uncertainty about the U.S. government's position on the GPA undermines international cooperation around secure and trusted 5G infrastructure because it would create space for major suppliers of ICT equipment to reorient their procurement strategies away from U.S. interests. Countries like China that have not joined the GPA would then benefit from such a weakened agreement.

**k. Shore up and expand the WTO Information Technology Agreement.**

The Information Technology Agreement (ITA) has significantly expanded global ICT trade and continues to play a vital role for the U.S. ICT industry by ensuring zero-duty treatment for many product categories that go into 5G deployment including semiconductors, semiconductor manufacturing and testing equipment, software, and scientific instruments. Since its enactment, the ITA has spurred two-way trade in ICT products, with one study attributing a 10% annual increase of ICT exports from 1996 to 2008 to the agreement.[11] The ITA has also bolstered the formation of an efficient global ICT chain that relies on collaboration among equipment supplies, network operators, and customers for ICT product deployment. By promoting trade and investment, the ITA has not only spurred innovation in the ICT industry but also has created a cost-competitive trusted network of manufacturers and distributors.

[11] Stephen J. Ezell, *The Benefits of ITA Expansion for Developing Countries*, Info. Tech. & Found. 2-3 (2012), http://www2.itif.org/2012-benefits-ita-developing-countries.pdf

The U.S. government should enforce compliance with ITA bound rates in its trade relations with other countries to encourage cooperation around secure and trust 5G networks. Many countries have in the past avoided their relevant ITA obligations and raised tariffs on covered ICT products. For example, India has levied duties on covered products on six separate occasions in violation of the basic WTO obligations on duty treatment documented in the country's General Agreement on Tariffs and Trade (GATT) schedule. The U.S. government should consider filing or joining WTO cases to address this problem as well as including compliance provisions with the ITA in various bilateral or plurilateral trade agreements.

In addition, the U.S. government should also support expanding the ITA to include more members in order to develop a secure and trusted 5G network that can operate globally and encompasses key players in the ICT industry. A trading system that is sensitive to cost-competitive mechanisms will give vendors and market participants more information to make informed decisions about the global ICT supply chain. These decisions, in turn, will help ensure that international actors act cooperatively with each other in determining the most trusted and secure 5G products and services.

**l. Expand existing export promotion programs and export credit efforts to support trusted manufacturers of ICT network equipment.**

The U.S. government should also utilize U.S. export promotion programs to focus on the ICT equipment sector. In order to encourage international cooperation around secure and trusted 5G networks, the U.S. ICT industry must participate in the market and develop relationships with vendors, network operators, and equipment suppliers across the world. This is best achieved when the U.S. actively engages at different levels of the value chain and promotes ICT exports. The U.S. government has a range of tools to facilitate market exports including the Market

Development Cooperator Program, the U.S. Foreign Commercial Service, U.S. Department of Commerce Certified Trade Missions, and other export promotion programs.

In addition, the U.S. government should also work with export credit agencies to focus on the ICT sector and fund exports accordingly. The Development Finance Corporation (DFC) and Export Import Bank (ExIm) both play a role in financing credit-intensive export projects abroad. ExIm has faced difficulties in terms of maintaining its funding stream and managing internal requirements on the types of projects that the organization can fund. The DFC, on the other hand, continues to develop their ICT-related work. With more consistency and flexibility, these agencies may better align funding programs to support ICT infrastructure projects and ensure that trusted manufacturers of network equipment can succeed in the international marketplace.

Export credit agencies should also leverage existing industry supply chain security frameworks in order to prioritize projects that secure a trusted 5G infrastructure. For example, TIA's supply chain security standards and measurement effort can aid these agencies in how they engage with and identify trustworthy ICT equipment suppliers. As these programs become more familiar with existing supply chain security frameworks, it will better help both industry and government adopt to changes in the international environment and accommodate best practices.

*WHAT OTHER ACTIONS SHOULD THE U.S. GOVERNMENT TAKE TO FULFILL THE POLICY GOALS OUTLINED IN THE ACT AND THE STRATEGY?*

**m. Expanding funding for NIST and ensure that it plays a leading role in coordinating federal agency engagement with the private sector.**

The National Institute of Standards and Technology (NIST) should play a leading role in coordinating federal agency engagement with the private sector when it comes to standards. In its current capacity, NIST is an important partner for the ICT sector, but lacks sufficient resources. The U.S. government should continue to support and encourage recent efforts by

NIST to strengthen the market-led private-public partnerships that underscore R&D initiatives across the country and create favorable environments for private investment.

## III. In order to ensure a successful 5G U.S. deployment, the Implementation Plan needs to continue to create a regulatory environment that fosters investment and innovation.

***Line of Effort One:*** *Facilitate Domestic 5G Rollout.*

*HOW CAN THE U.S. GOVERNMENT BEST FACILITATE THE DOMESTIC ROLLOUT OF 5G TECHNOLOGIES AND THE DEPLOYMENT OF A ROBUST DOMESTIC 5G COMMERCIAL ECOSYSTEMS?*

### a. Any national strategy on 5G should continue the U.S. government's work on freeing up valuable mid-band spectrum.

In order for the U.S. to maintain its role as a global leader in 5G, the Administration must continuously work in tandem with industry to repurpose high-demand spectrum for private and public-private joint use. Over the last half-decade, Congress has recognized the need for stronger and more widespread connectivity. Developments in innovation and investment, thanks in a large part to actions taken by Congress in the Spectrum Pipeline and MOBILE NOW Acts,[12] have accelerated nationwide efforts to reinvent spectrum allocation to promote sector growth. For example, TIA commends the FCC's most recent work in the 5G Fast Plan, which represents an encouraging framework that helps to unleash the power, ingenuity, and investment through use of highly coveted spectrum options largely and previously unavailable to non-incumbent entities.

The Implementation Plan should continue this heightened focus on potentially reallocating other bands of valuable mid-band spectrum. NTIA has already facilitated this with

[12] MOBILE NOW Act, S.19, 115 Cong. (2017) (passed under the RAY BAUM's Act of 2018).

the release of the Sharing Report on the technical feasibility of sharing in the 3.45 GHz band. In an already crowded and limited field of spectrum, this band has become increasingly valuable due to its ability to support precise 5G throughput and latency requirements.

Realizing that previous and ongoing incumbent use of this band and others holds considerable importance to the federal government, TIA suggests that NTIA continues to work with various government incumbents on further bands for reallocation.

**b. Continued ICT investment and the deployment of 5G requires regulatory certainty.**

In order to ensure the deployment of a robust domestic 5G commercial ecosystem, policymakers must provide certainty as to what rules will regulate the 5G industry over the long-term. As the ICT industry will invest significant resources to meet regulatory requirements set by the U.S. government, abrupt changes to 5G-related policies could increase transaction costs for firms, hinder the domestic rollout of 5G technologies, and ultimately harm the U.S.'s efforts to maintain its position as a global leader in 5G.

To this end, the Implementation Plan should offer a light-touch approach when it comes to regulation to incentivize 5G deployment in the marketplace and avoid stifling private industry with uncertain and unpredictable policy commitments. This light-touch approach should remove unnecessary regulatory or market access barriers that force companies to direct funds to regulatory compliance issues instead of 5G deployment. In addition, by making regulatory requirements flexible and not subject to abrupt change, the U.S. government would ensure an environment that encourages investment and promotes 5G innovation.

### c. U.S. government should review existing research and development projects for potential public participation.

The ICT industry partners building the global 5G networks and the IoT devices that run on them are engaged in numerous research and development projects. These R&D efforts focus on numerous use cases that can be addressed by 5G, which utilizes a wide range of spectrum and has operational capabilities far beyond what was offered by 4G. For this reason, TIA urges the U.S. government to be active in working with industry and participating in R&D efforts going forward. While not purporting to be an exhaustive list, some efforts the Administration could consider participating in include:

i. Efforts to utilize machine learning artificial intelligence to increase radio spectrum efficiency.[13]

ii. Technological advances that push towards a more efficient use of spectrum, such as beam forming.

iii. Cost-effective ways to make spectrum sharing more efficient without causing additional interference.

iv. Radio wave behavior at terahertz frequencies.[14]

U.S. government participation in these and other similar efforts not only will assist industry in charting the future course of 5G deployments, but also further the understanding of radio systems generally as the need for spectrum continues to grow. Additionally, in order to

[13] *The Radio Frequency Spectrum + Machine Learning = A New Wave in Radio Technology*, Def. Advanced Res. Projects Agency (DARPA) (Aug. 11, 2017), https://www.darpa.mil/news-events/2017-08-11a; *How AI Is Starting to Influence Wireless Communications*, IEEE Spectrum, https://spectrum.ieee.org/computing/software/how-ai-is-starting-to-influence-wireless-communications

[14] While the FCC opened this up for commercial use, R&D could help accelerate industry's understanding of how to put the spectrum to productive use.

spurn industry investment, TIA urges U.S. government to partner with industry and identify areas where generating public-private use cases could inform some of the positive changes that 5G growth will promote.

## IV. Conclusion

TIA welcomes this initial opportunity to discuss the ICT industry's priorities for the Administration, as part of this effort to create a comprehensive federal strategy to safely and securely deploying 5G. Our member companies work every day to ensure that next generation networks, devices, and services are deployed as efficiently and safely as possible, and TIA is proud to be able to advocate on behalf of the ICT industry on the important work of the Implementation Plan. We welcome any future opportunities to discuss the foregoing policies and the completion of the Implementation Plan.

By:

Colin Black Andrews
Director, Government Affairs

Patrick Lozada
Director, Global Policy

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

Filed: June 25, 2020