Telecommunications Industry Association
1310 North Courthouse Road, Suite 890
Arlington, VA 22201 | www.tiaonline.org

October 30, 2025

Via online submission at www.regulations.gov

Edward Marcus
Chair, Trade Policy Staff Committee
Office of the United States Trade Representative
604 17th Street NW
Washington, DC 20508

RE: Docket Number USTR-2025-0016, Request for Comments on Significant Foreign Trade Barriers for the 2026 National Trade Estimate Report

Dear Mr. Marcus:

We appreciate the opportunity to submit the enclosed comments regarding the 2024 National Trade Estimate Report on Foreign Trade Barriers ("NTE"), as well as comments regarding the operation, effectiveness, and implementation of, and compliance with U.S. telecommunications trade agreements pursuant to statute ("Section 1377").

The Telecommunications Industry Association (TIA) represents approximately 400 manufacturers and suppliers of high-tech telecommunications networks and services here in the United States and around the world. TIA is also an ANSI-accredited standards development organization.

As in past years, our comments will highlight trade barriers that TIA members face across a range of economies as well as barriers to digital trade across America's trading partners. Digital trade supports American workers, and we believe it is more important than ever that USTR push back against efforts by China and others to mandate source code disclosure, discriminate against the purchase of digital products based on country, obstruct cross-border data flows, and impose data localization mandates.

If you have any questions about this document or if we can assist you in other ways, please do not hesitate to contact Colin Andrews at 202-365-4027 or at candrews@tiaonline.org.

Sincerely,

Colin Andrews
Senior Director of Government Affairs

Telecommunications Industry Association
2026 NTE and Section 1377 Comments
Docket Number USTR-2024-0015
October 30, 2025

Contents

BRAZIL

Protectionist Measures Favoring Domestic ICT Industry

Brazil provides tax reductions and exemptions on many domestically produced ICT and digital goods that qualify for status under the Basic Production Process (*Processo Produtivo Básico*, or PPB). The PPB and I.T. law were reshaped after being considered inconsistent under WTO rules (Dispute Settlement decisions -- WT/DS472/R and WT/DS497/R, Brazil – Certain Measures Concerning Taxation and Charges). Despite this reshaping, the measures still require local content, albeit in a less straightforward way than previously. Tax exemptions are also provided for the development and build-out of telecommunications broadband networks that utilize locally developed products and investments under the Special Taxation Regime for the National Broadband Installation Program for Telecommunication Networks (*Regime Especial de Tributação do Programa de Banda Larga para Implantação de Redes de Telecomunicações,* or REPNBL-Redes).

Another example of localization requirements that impose barriers to trade is the bidding for spectrum bands promoted by the Brazilian National Agency of Telecommunications (*Anatel*) in June 2012. Companies that were given the right to explore the 2.5 GHz and 450 MHz spectrum bands were required to prove investments that include a high percentage of products, equipment, and telecommunication systems with local content. This includes goods manufactured in Brazil according to the PPB rules and locally developed technology.

Recommendation: TIA is of the view that the government of Brazil should adopt measures that foster more competitiveness in terms of local content instead of just imposing requirements. It should eliminate policies that may obstruct fair access to the future spectrum auction processes for foreign companies. TIA also recommends that the methodology for software certification for local development be rescinded as a tool to grow and develop Brazil's domestic software industry. We recommend the government of Brazil not unnecessarily impede the cross-border flow of information through local data storage mandates. Market dynamics, not government requirements, should be the main factors determining which technologies should be deployed based on customer needs. Brazilian consumers, including government agencies and businesses, should benefit from competition and have access to world-class technologies, regardless of where they are produced.

Government Procurement

Decree 7174/2010, which regulates the procurement of a number of goods including ICT goods and services, allows federal agencies and state entities to give preferential treatment to locally manufactured products and goods or services with technology developed in Brazil based on compliance with the PPB. ICT bids for goods and services considered "strategic" may be limited to those with technology developed in Brazil.

Recommendation: Brazil should continue to move forward in its bid to accede to the WTO Government Procurement Agreement (GPA) in order to increase transparency in the procurement process. This would help address concerns regarding preferential treatment and promote fair competition.

Complex Tax and Tariff System

Brazil places high import tariffs on imported telecommunications products, including a 16 percent import tax on mobile phones, and a system of multiple cascading taxes makes the effective tax rate much higher. Double taxation is an issue that affects many multinational companies doing business in Brazil, even those headquartered in countries with which Brazil has a Bilateral Tax Treaty in effect. While the multiple layers and cumulative nature of taxation in Brazil is a cross-sectoral challenge, there are special complexities regarding taxes on telecom services, which reach as high as 40 percent in some states. A variety of tax incentives disadvantage foreign goods and favor domestically produced products. Brazil's complex tax system often leads to litigation, and there is currently no process for mediation.

Recommendation: Brazil should explore simplifying its tax system to better align it with other countries. As is, the current unnecessarily complicated tax system leads to higher prices that are subsequently passed on to consumers. Brazil should also streamline the legal process under which taxpayers can challenge assessments raised by the Brazilian tax authorities, which should include the implementation of a tax mediation procedure.

Brazil should also join the WTO Information Technology Agreement (ITA). The ITA removes tariffs on a broad range of ICT products, including telecommunications equipment. This would reduce costs for consumers, expand connectivity, and drive broader economic growth.

Testing and Certification

TIA is concerned about the Brazil National Telecommunications Agency (*Anatel*) not accepting test data generated outside of Brazil, except in those cases where the equipment is physically too large and/or costly to transport. The limitations on test data essentially requires virtually all testing for I.T./telecom equipment, including everything from mobile phones to optical cables, to be conducted in Brazil. Test data is only accepted when it is generated by a laboratory located in Brazil, and when witnessed by an approved certification body. These requirements conflict with Brazil's WTO commitments, including the WTO TBT Agreement, Article 2, Section 2.2, by creating unnecessary barriers to international trade, which raise costs and delay time to market. For example, one member company reported that Brazil currently requires them to ship 64 battery packs for testing for each new product to labs in Brazil. However, restrictions on the air transport of lithium-ion battery packs because of a perception that they are dangerous have caused significant delays and substantial cost for companies seeking to sell battery-powered ICT equipment in Brazil. Certification delays can take three to four months, without any increase in value to Brazilian consumers, and in many cases must be undertaken every two years.

Recommendation: *Anatel* should institute reforms that allow manufacturers to manage their own test process to minimize cost and redundancy and declare conformity with Brazilian requirements in the manner described in ISO/IEC 17050 Part 1 and Part 2. *Anatel* could then focus more attention on enforcement and less on equipment certification. This would help to ensure Brazilian consumers have access to innovative products more quickly and at a lower cost.

ICT Device Pre-Import Certification

Regulation on Conformity Assessment and Approval of Telecommunications Products (Resolution No. 715, of October 23, 2019) prohibits the use and marketing in Brazil of non-approved telecommunications products. In 2020, Act n. 4521 (2020) was published that requires all certificated

telecom products to be homologated prior to importation, except for lab testing, in effect as of December 27, 2021. Samples for other local tests and prototypes are under specific authorizations (for Temporary Use of Spectrum or for Special Service for Scientific and Experimental Purposes). These processes are not clear and the timing to grant approval is estimated from 60 to 90 days.

Recommendation: USTR should encourage the improvement of such regulation to require only minimal information to ensure the level of confidentiality needed, especially for prototypes. In addition, to facilitate the import of products and investment in Brazil, the import process should allow entry of reasonable quantities and should be compatible with global company operations.

Mutual Recognition Agreements

The United States has urged Brazil to implement the Inter-American Telecommunication Commission (CITEL) Mutual Recognition Agreement (MRA) with respect to the United States. Under the CITEL MRA, two or more CITEL participants may agree to provide for the mutual recognition of conformity assessment bodies and mutual acceptance of the results of testing and equipment certification procedures for imported telecommunications equipment. The United States and Brazil are both participants in CITEL. If Brazil implemented the CITEL MRA, it would benefit laboratories in both countries that could test to the other country's specifications, suppliers seeking to sell telecommunications equipment globally, and consumers who would enjoy speedier access to new technologies.

Recommendation: Brazil should implement the CITEL MRA. Implementation of the MRA would benefit U.S. suppliers seeking to sell telecommunications equipment in the Brazilian market by allowing them to have their products tested in the United States to meet Brazil's technical requirements, eliminating the need for such testing at laboratories in Brazil.

Remanufactured Goods:

Brazil is one of the few countries in the Western Hemisphere that does not allow the importation of remanufactured goods. The Ministry of Economy issued a Public Consultation (circular Secex 45/2021) on July 2021 to collect information and investigate the potential impacts on the economy, industry, investments, employment and environment if Brazil were to allow the importation of remanufactured goods. This policy is creates a burden to companies and consumers alike because refurbished products and components are “like new” products and should not be banned. U.S. companies are required to continue supporting customers with products that are under warranty, especially when such products have reached end-of-sale, and components are no longer available as new products.

Recommendation: USTR should encourage Brazil to allow for the import of remanufactured goods and parts, which can reduce the consumer cost and company service costs of such goods, and help advance environmental goals by facilitating a more circular economy.

CAMBODIA

Local Testing Requirements

The Telecommunications Regulator of Cambodia (“TRC”) is responsible for overseeing the “type approval” process for telecommunications equipment. Type approval is required to import

telecommunications products and includes review of foreign standard test reports. The TRC imposes a variety of type approval and regulatory requirements, including enforcing country-of-origin requirements (e.g., separate certification needed for each country-of-origin for the same model of the product). In particular, the TRC requires suppliers to acquire test reports in the vendors' name in Cambodia for Small Form-factor Pluggable ("SFP") modules that typically do not require certification in other countries. Reports from Original Equipment Manufacturers ("OEMs") or Original Design Manufacturers ("ODMs") are not accepted by the TRC. Additionally, type approval is required for line-cards (also not required in other countries). The current regulations are highly burdensome for U.S. suppliers because it is impractical to obtain certificates and type approval for line cards that cannot function independently. Lastly, the TRC also prohibits import of refurbished products.

The TRC's overly stringent enforcement of its type-approval guidelines acts as a market access barrier that is out-of-step with practices in other countries' regulations and disrupts business operations and customer support in Cambodia. Furthermore, Cambodia made significant expansions to the scope of type approval without consultation or provision of transition periods.

Recommendation: TRC should revise its type approval process for ICT equipment so that these processes do not unnecessarily increase consumer costs and are better aligned with the commercial realities of global supply chains. For instance, we encourage TRC to accept OEM and ODM reports and accept internationally-recognized standards to be used in such testing. Such an approach allows for robust security vetting without imposing new fees that will drive up end user costs or needlessly delay time to market for ICT products.

CANADA

Canada is a member of the WTO Government Procurement Agreement ("GPA"), which binds Members, including the United States and Canada, to reciprocal market access in government procurement. Shared Services Canada ("SSC"), a government agency that was formed in August of 2011, has not been listed in Canada's Appendix I Annexes of the WTO GPA. SCC is the Canadian government's largest procurer of information technology ("IT") products and services, as it brings together the IT resources from 42 departments.

Recommendation: Given its impact on the ICT sector, Canada should list the SSC in the Appendix I Annexes of the WTO GPA.

CHILE

Need Public Consultation on Regulatory Requirements

Over the past three years, Chile has implemented a number of regulations, guidelines and technical requirements that disrupt global supply chains, resulting in product delays and increasing the cost of doing business. Such requirements are often Chile-specific obligations that are inconsistent with global practices or standards. In a number of cases, they appear to have been published without seeking public input. The resulting costs and challenges to business could arguably have been avoided with prior industry consultation.

Recommendation: Chile should provide a public consultation process with affected stakeholders prior to finalizing and enacting regulation. This will offer the industry an opportunity to bring useful feedback and experience into the regulatory process.

Homologation Issues

In March 2017, Subtel Resolutions 1474 and 1463 (and updates) imposed a mandatory Chile-unique emergency alert (vibration) standard on all mobile devices. In addition to the required software changes, companies also must test phones *from every shipment* for compliance in a lab in Chile or establish local testing labs.

These requirements are unduly burdensome and/or unnecessary. No other country requires this type of per shipment testing and hardest hit may be SMEs that do not import in bulk and importers facing import delays. To the extent that Subtel believes such a measure is needed, it would be sufficient to require testing for a new software/major upgrade and/or authorize random inspections to deter evasion.

Recommendation: SUBTEL should revise the existing processes for testing, inspection, and registration associated with the homologation of telecommunications equipment so that such processes do not unnecessarily increase consumer costs and are better aligned with the commercial realities of global supply chains.

Mobile Phone Label Requirements

In July 2017, SUBTEL issued guidelines, "Manual of Graphic Standards: Broadband Label" pursuant to Resolution Nº 1.463. All mobile phone sellers must include a specific label on their packaging and in certain advertising indicating that device's compatibility with all mobile networks (e.g. 2G, 3G, 4G). The label is required for all phones and further delineate the label specifications, including content, colors, size, and placement.

Recommendation: SUBTEL should limit or remove national labeling requirements and instead align with global labelling standards, including the use of e-labels.

Safety Marking

Chile's Resolution 16677/2017 and protocol PE-8/8 implemented new safety certifications named "System 2" (S-mark System) requiring that all power adaptors for smartphones to be certified in Chile by the SEC (*Superintendencia de Electridad y Combustibles*) and that these certifications be displayed with the product that contains the charger. In mid-2019, Chile also issued Public Consultation PE Nº 8/9:2019, regarding the extension of the rule for many other power adaptors including for notebooks, tablets, and audio and video products. These regulation and protocols have created challenges and cost increases for OEMs and sellers who only had a short period of time to comply with this Chile-specific requirement.

Recommendation. SEC should accept international documentation issued under the C.B. scheme by accredited international bodies certifying product safety instead of mandating duplicative, Chile-specific requirements with unnecessary factory inspection rules.

CHINA

State Campaign to Replace Foreign Technology with Domestic Products

Despite ostensibly agreeing to ramp up the purchase of U.S. ICT telecommunications equipment as part of purchase targets set out in the "Phase One" trade deal agreed to in early 2020, the Chinese government has continued to pursue an aggressive import substitution campaign in key sectors such as telecommunications equipment, semiconductors, software, cloud computing, and artificial intelligence. President Xi Jinping and other senior officials continue to promote technological "self-reliance," advancing a range of measures to support domestic industry and undermine global technology companies. U.S. firms have been particularly impacted by these efforts in the context of rising U.S.-China trade tensions.

This industrial policy, previously advanced under the name "Made in China 2025," is now being pushed forward under the label of the Strategic and Emerging Industries (SEI) initiative. This initiative dates back to planning documents released in 2010 and represents primarily a continuation of previous technology industrial policies as opposed to a substantive change from the Made in China 2025 initiative.

Over the past several years, government agencies have issued a growing number of guidelines and policies that call on both companies and government entities to buy I.T. hardware that is "secure and controllable," "secure and trustworthy," or "indigenous and controllable." Though Beijing has never provided a clear definition for these terms, Chinese officials have invoked such language in state media to explain China's need to develop indigenous technology and to justify cybersecurity reviews of I.T. products.

These restrictions have notably increased in the past few years through both formal and informal restrictions on the purchase of non-Chinese technology generally and U.S. technology specifically. Examples include:

- Informal guidance issued to Chinese government entities and SOEs to avoid purchasing ICT equipment from U.S. companies;
- Threats issued publicly in state media outlets to interrupt individual company operations in China;
- Guidance issued by city and provincial governments requiring computer purchases to incorporate domestically manufactured inputs such as computer chips;
- Laws, rules, and standards requiring entities classified as "Critical Information Infrastructure" limit the use of products who supply could be disrupted due to "non-technical factors like policy, diplomacy, and trade."

The Chinese government has also continued to release a maze of overlapping laws, rules, and standards it says are necessary for national security, many associated with the Cybersecurity Law that took effect in June 2017. TIA is concerned that China's growing slate of security rules may disadvantage U.S. exporters selling into China's commercial markets. With penalties set to increase, the practical impact of these restrictions are likely to increase even further in the near future. These “secure and controllable” standards remain an issue, and are not transparent for American or trusted companies.

Discriminatory Regulations and Standards Ostensibly Based on National Security.

Beijing has sought to project its security umbrella far beyond areas where valid national security concerns might normally apply to include large swathes of the economy. The Chinese government has shown itself increasingly inclined to categorize commercial industries as Critical Information Infrastructure (CII), which it uses to justify restrictions on public communication and information services, energy, transportation, water conservancy, finance, public services and e-government. The scope of this system became clearer with the release of Critical Information Infrastructure Security Protection Regulations which came into effect in September of 2021.

Since the implementation of the Cybersecurity Law, China has issued a complex and overlapping series of policies and standards that restrict the ability of global companies to access the China market. China's Technical Committee 260 and other Chinese standards development bodies have significantly increased the pace of the release of these documents over the course the previous few years. China has plans to further expand the scope of ostensibly cybersecurity-focused standards over the next few years per the "Guidelines for the Development of Data Security Standard System in Telecom Network and Internet Industry," which also contains a length list of relevant standards of concern to industry.

***Recommendation**:* China should narrowly limit the scope of CII to networks involved in operations critical to national security, fully open technical committees responsible for developing security standards to participation by non-Chinese entities, and eliminate language that discriminates against foreign firms.

Restrictions on Cross-border Data Flows

China has aggressively expanded its restriction on crossborder data flows over the last few years including through the promulgation of a series of laws, rules, and standards.

These various actions have solidified the crossborder data restrictions laid out in China's Cybersecurity Law and continue to make it challenging for multinational companies to do business in the country.

Recommendation: The development of e-commerce, innovation, and overall economic growth in the digital era – all key objectives of China's Internet Plus strategy -- are enabled by the free flow of data across borders. Instead of pursuing an overly restrictive, China-specific scheme of data containment, we would recommend Beijing seek to align with international practice in how it approaches data. The Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system and the Organization for Economic Co-operation and Development (OECD) Privacy Principles could serve as key references in the development of frameworks would help to enable interoperability and compatibility with respect to data. We strongly urge China not to impose onerous restrictions on cross-border data transfers.

Expansion of Security Ranking System

The Chinese government has expanded and updated a security ranking system, known as the Multi-level Protection Scheme (MLPS). Under the MLPS, networks are assessed according to a subjective ranking based on their alleged sensitivity to national security, social order, the public interest, and the legitimate interests of individuals and organizations. Networks classified above a level 3 on a scale of 1 to 5 will be required to use more "secure" products and services. It is not clear how security would be evaluated,

raising concerns that the rules will be interpreted to favor Chinese suppliers. Expanded MLPS 2.0 rules came into effect in December of 2019, and further expanded the scope of this ranking system.

Recommendation: TIA urges the Chinese government to refrain from implementing security policies that unfairly limit the use of global ICT solutions by companies on security grounds.

Cybersecurity Review Regime

China's Cybersecurity Review Measures, which came into effect in June of 2020 after several rounds of edits and were subsequently revised in July of 2021, discriminates against use of foreign ICT products in China by enterprises identified as "Critical Information Infrastructure."

Specifically, Article 9 of the law contains language which are likely to exclude the use of foreign products by identifying the "the risk of supply disruptions due to political, diplomatic, and trade factors." This is most likely to impact U.S.-origin technology specifically because of company compliance with U.S. export control rules. Article 9 also creates uncertainty with a vague catch-all category of "other factors that could harm CII security and national security."

The 2021 revisions to the Measures also added a vague new category of covered network products and services called "important telecommunications products." As this is not a defined product category and many types of ICT products and services are already explicitly covered, the addition of this category creates uncertainty about a wide range of ICT sales and whether they would be covered under the Measures.

Recommendation: We recommend that implementation of the Cybersecurity Review Regime be scoped narrowly and use risk-based assessment criteria that do not discriminate against products produced by non-Chinese companies.

Full Market Access for Products Listed in Telecommunications Services Catalogue

China's 2019 update to the Telecommunications Service Catalogue continues to impose significant market access restrictions on some of the fastest growing and most important technology sectors. This impacts cloud computing, where U.S. companies have staked out a leading role, as well as a number of other digital services including content delivery networks, information services and virtual private networks.

The catalog incorrectly classifies a wide range of ICT technologies and services as telecom value-added services, when in fact they are computer and related services that are merely delivered over a telecom network. This distinction matters because companies that provide so-called value-added services can only operate in China through joint ventures, in which foreign ownership is capped at 50 percent. In reality, they should be classified as computer and related services, which under China's WTO commitments should not be subject to any market restrictions.

The regulation requires TIA member companies that seek to do business in these areas either to find a Chinese partner, which brings its own set of challenges, or choose to stay out of the market altogether.

The resulting disparity in treatment between China and the United States is particularly noticeable in the cloud market. Chinese cloud providers are expanding globally into geographies including the U.S., where they are allowed to freely establish commercial operations without need of a license or foreign partner.

MIIT's October 7 draft plan to "open up" the value added telecommunications service catalog – announced in early October – does not create meaningful opportunities for TIA members as it is limited in scope.

Recommendation: TIA urges MIIT to dismantle the value-added telecom services licensing regime, including associated equity caps and capitalization requirements. We seek to ensure that efforts to regulate services delivered over public networks be consistent with China's WTO commitments.

Standards-setting Approaches that Depart from Global Norms

Article 15 of China's revised 2019 Foreign Investment Law (FIL) marked rhetorical progress in the ability of foreign enterprises to participate in standards development in China. This rhetorical progress, however, has not been matched by results. While U.S. companies are able to participate in some cases, in many others they continue to be excluded from participation in government-affiliated working groups deemed sensitive by the Chinese government. In other cases, companies are able to join certain standards development technical committees but are subsequently excluded from certain working groups.

More broadly, progress is undermined by the reality of a Chinese standards-setting regime that has traditionally distinguished between Chinese and non-Chinese participants, undermining the core principle of "openness without discrimination" in standards policy outlined in the WTO Technical Barriers to Trade Committee in its "Decision…on Principles for the Development of International Standards."

Finally, it is unclear the extent to which foreign companies will be able to fully participate in the development "social organization standards," which are primarily generated by groups of Chinese companies and may later be incorporated into Chinese laws and regulations.

Measures implementing key provisions of China's revised *Standardization Law* also continue to raise concerns in the U.S. business community. For example, requirements that companies disclose "enterprise standards" in effect require companies to share proprietary product or service specifications. These details often contain confidential patents, copyrights, and trade secrets which are protected by a range of intellectual property rights.

Over the past few years, China has released a series of documents laying out its plans for future engagement on standards issues most notably the "National Standards Development Outline" and an ensuing implementation plan earlier last year. While there are some individual statements in the outline and implementation plan indicating openness to international standards, there are also indications that China is set to continue to leverage industrial policy to improperly influence standards developments through subsidies and a government "coordination mechanism" that will support PRC government and industrial policy priorities.

Recommendation: We ask that China fully implement its commitment in the FIL to allow for full foreign participation in Chinese standards technical committees. We also ask that China employ international

standards as the basis for mandatory standards whenever possible, align with global rules and best practices regarding independent company participation in SDO activities, provide adequate time for comment on new draft standards, limit disclosure requirements and unfair treatment related to the implementation of the enterprise standards system, and ensure that social organization standards are not incorporated into Chinese laws and regulations in such a way that creates market access barriers for foreign companies.

Testing and Certification

The product testing and certification process in China is significantly more difficult than in other markets, which increases the costs of U.S. products for sale in the Chinese market. China's current certification requirements for telecommunications equipment conflict with its WTO obligations, which stipulate that imported products should be subject to only one conformity assessment scheme and require the same mark to be used for all products (Article 13.4(a) of China's WTO Accession). In total, China has three different licensing regimes – the Radio Type Approval (RTA), the Network Access License (NAL), and the China Compulsory Certification (CCC). For a given piece of equipment, it can cost between U.S. $20,000-$30,000 to test for all three licenses (RTA, NAL, and CCC).

China has opted out of the C.B. scheme for electromagnetic compatibility (EMC) testing, with the result that such testing must be done in-country. EMC requirements emerged out of a collective international effort and many countries participate in the EMC component of the certification body (C.B.) scheme and accept C.B. scheme test reports generated by other participating members.

Ideally, China should eliminate the NAL as a product licensing requirement. However, recognizing the structural/legal problems that would pose, TIA and its members recommend that, in the interim, China reduce the number of tests required by the NAL to a bare minimum.

To promote improved transparency in testing and certification in China, reduce associated costs and generally facilitate trade, we urge the Chinese government to provide the necessary scope in product coverage and enact the necessary legislative changes to allow it to resume meaningful talks with the U.S. government on a mutual recognition agreement (MRA).

Recommendation: TIA asks the government of China to improve the application of international conformity body scheme reports by national laboratories and eliminate the need for additional samples and redundant testing. Any certification-related process should be in conformance with related WTO TBT requirements. We also recommend that such efforts conform to international best practices as reflected in the ISO/IEC CASCO Guidelines. Finally, we strongly encourage China to take steps to make meaningful progress on an MRA.

Anti-Monopoly Law

TIA notes the purpose of China's *Anti-Monopoly Law* (AML), which took effect in 2008, is to prevent monopolistic behavior and enhance competition in China's commercial environment. While this is a laudable goal, AML investigations by Chinese authorities appear to be distorting the AML and related laws to target foreign companies as an additional policy tool to support China's national industrial policy objectives. The Chinese companies that benefit from these AML enforcement cases are often national champions in various strategic sectors, including the telecommunications sector.

Recommendation: TIA urges the government to employ the AML only in such a manner as to promote fair and open competition without trespassing on I.P. protections or otherwise undermining the market position of foreign companies to the advantage of domestic entities.

Government Procurement

China's progress towards joining the WTO Government Procurement Agreement (GPA) has been extremely slow, dating from its first offer for accession in December 2007 to its most recent revised offer (its sixth) submitted in October 2019, which unfortunately fell short of expectations in its coverage. In the meantime, as noted earlier, the government has issued a number of policies under the banner of improving security that seek to replace foreign ICT goods and services with "secure and controllable" Chinese products in government computer systems. Such actions raise questions about the current degree of Chinese political support for improving the terms of any subsequent GPA offer. However, we believe China would benefit from embracing the principles of openness, transparency and non-discrimination embodied in the GPA.

Recommendation: TIA urges China to join the GPA and ensure that its accession package fully accords with international norms.

Encryption Requirements

China's 2019 Cryptography Law includes restrictive requirements for commercial encryption products that "involve national security, the national economy and public interest" which must undergo a security assessment, including critical information infrastructure. This has resulted in unnecessary restrictions on foreign ICT products and services.

Recent regulations have added to concerns that China's encryption requirements are being used to discriminate against American companies. For example, China amended the Commercial Cryptography Administrative Regulations in April 2023. The amended regulations fail to support interoperable international standards and use internationally standardized encryption algorithms. Furthermore, the regulations reflect an extensive import license/export control scheme and impose requirements applicable only to CII and party and government organs to networks above Multi-Level Protection Scheme ("MLPS") level three.

Furthermore, on October 7, 2023, the State Cryptography Administration ("SCA") published the Administrative Measures for Security Assessment of Commercial Cryptography Applications (Measures), which came into effect on November 1, 2023. The measures proposed the concept of Important Network and Information Systems without providing definitions. Unless these important ambiguities are favorably resolved, these regulations will impose significant compliance costs and create entry barriers for American companies that rely on internationally accepted encryption algorithms.

Recommendation: TIA urges China to support interoperable international standards and standardized encryption algorithms to avoid high compliance costs for companies located out of country.

Restrictions on Cloud Computing

Even though U.S. cloud service providers ("CSPs") have stimulated innovation and application of cloud services around the world, China's regulators impose market access restrictions for foreign companies,

which require Value-Added Telecoms ("VAT") licenses. China has launched "pilot" programs to open its cloud market in Beijing, Shanghai, Shenzhen and Hainan "free trade zones," but CSPs still need to fulfil the previous localization requirement. These burdensome restrictions are exacerbated by other market access restrictions: connectivity requirements, restrictions on the ability to engage in cross-border data transfers, and requirements to localize computing infrastructure

Recommendation: TIA urges China to revise these pilot free trade zones to allow CSPs to operate without fulfilling the previous localization requirements.

COLOMBIA

VAT Application

Colombia currently offers a VAT exemption for computers and other computing devices below a specified price, equivalent to 50 UVTs, or COP 1,780,350 in 2020. A similar provision applies for tablets and smartphones if the price falls below the 22 UVTs, or COP 783,354 in 2020. Besides the artificial threshold of the policy, which makes the most advanced devices less accessible to the Colombian population, exchange rate variations make the market highly unpredictable. In 2019, for example, the dollar equivalent of 50 UVTs varied from a low of US$480 to US$560. This introduces a considerable element of uncertainty for small and medium business owners who retail such devices, since they are captive to the vagaries of the exchange rate. Whether or not a device vendor must pay the steep 19 percent VAT surcharge depends on currency fluctuations on the day a given device is imported.

Today, smartphones (or intelligent mobile devices) often substitute for such devices, but are still subject to the full 19% VAT rate if their price is higher than 22 UVTs. Intelligent mobile devices or smartphones (e.g. mobile phones that offer greater functionalities than feature phones) should be afforded the same VAT exemption as other computing devices. Failure to afford the VAT exemption has the potential to restrict electronic commerce and is a barrier based on the type of device, rather than its functionalities.

Recommendation: The Colombian government should extend the VAT exemption to apply to all smartphones as well as other digital devices.

Public Consultation on Regulatory Requirements

Over the past two years, Colombia has implemented a number of regulations, guidelines and technical requirements that disrupt global supply chains, result in product delays, and increase the cost of doing business. Such requirements are often Colombia-specific obligations that are inconsistent with global practices or standards.

In a number of cases, these regulations appear to have been published without seeking public input. Some agencies failed to conduct an impact regulatory analysis in its regulations, such as the Superintendency of Industry and Commerce, which is in charge of competition issues, consumer protection, and data protection.

Recommendation: Colombia should provide a public consultation process with affected stakeholders prior to finalizing and enacting regulations, particularly for Superintendencies that have rule-making

authority but are not bound by the rules applicable to the Regulatory Commissions. This will offer industry an opportunity to bring important feedback and experience into the regulatory process.

Theft of Mobile Phones

On October 16th, 2015, the Government of Colombia published Decree 2025, which "establishes measures to control the import and export of intelligent mobile phones, cellular mobile phones, and their parts, susceptible to classification under Customs Tariff subheading 8517.12.00.00 and 8517.70.00.00", as part of its strategy to address the theft of mobile phones. In practice, Decree 2025 creates burdensome restrictions and administrative requirements for trade in mobile phones, without significantly deterring or limiting illegal trade in stolen phones.

Implementation of the Decree continues to be disruptive to businesses, as the time frames set out in the law are routinely not met and no single agency owned responsibility for addressing such shortcomings. While several sets of changes were made to the Decree over the course of 2016, it still includes provisions that impede regular trade and commerce.

Colombia maintains a system of black (mobile phones reported as lost or stolen) and white (mobile phones with homologation, valid International Mobile Equipment Identity - IMEI) lists. It requires that each mobile phone have a government-issued verification certificate at the time of import. It requires exports (e.g., as WEEE or for repair) be on the White List, though not all phones must be included on that list prior to import – for example, a device brought into the country by an individual. This system is challenging the operational capacity of the government and recently civil society organizations raised privacy and security concerns about the system. While the concern about phone theft is valid, the current system imposes unnecessary and undue burdens and impedes regular trade and commerce of communications devices.

Rather than continue to address legitimate concerns about phone theft through processes that are not working, Colombia should explore approaches that have proven effective in other countries. These could include focused efforts on the illicit spare parts market, educational campaigns about technology-based solutions (such as those that allow the user to block the phone, remotely erase the content, and make the devices unable to connect to the network), and cooperation beyond national borders.

In 2019, the Communications Regulatory Commission (CRC) launched a general Regulatory Impact Analysis on these measures. It is expected that this analysis will show minimal effectiveness and additional burdens from this regulation on the industry. During 2020, though CRC has demonstrated little progress in developing this analysis.

Recommendation: We recommend the government repeal the import requirement to register all IMEI numbers before import and instead focus police enforcement on the places where organized crime tampers with IMEI systems.

Mobile Phone Label Requirements

In November 2019, the Superintendency of Industry and Commerce (SIC), acting as the consumer protection authority, issued regulation (Circular Externa No. 002 – November 2019) asking all mobile phone sellers and manufacturers to include a specific label on their packaging and in certain advertising indicating that device's compatibility with all mobile networks (e.g. 2G, 3G, 4G). The label is required for

all phones. The draft guidelines further delineate the label specifications, including content, colors, size, and placement. Labels must be placed on the front of the mobile terminal equipment packaging, in places either online or in-store, where they are exhibited, and when nontraditional or remote selling methods are used. In addition, sales representatives have to provide this information to potential buyers.

Requiring country-unique labels requires suppliers to exactly predict market demand, with the likely consequence that they will underestimate the supply available in a country. Specifically, on packaging, consumers often do not see packaging until after they have purchased a device so a label has no informational value. Analyses have shown that the label is most effective when displayed in the Point-of-Sale and online sites, but it has lower effectiveness when displayed in the packaging box.

A public consultation period of longer than two weeks and a regulatory impact analysis in this case might have explained what market failure was intended to be corrected by this regulation. It is important for any transparency policy to have a main objective that advances the public interest, which may be different from merely providing information to customers

Recommendation: SIC should revise its regulation and limit pervasive labelling mandates. TIA also supports the use of global standards for e-labelling.

EGYPT

Duties Imposed in Contravention of WTO Commitments

In November 2021, Egypt adopted a 10% tariff on imports of mobile phones ((Presidential Decision 558/2021), in contravention of Egypt's commitments under the WTO Information Technology Agreement. Notably, in addition to the 10% duty, Egypt also imposes a variety of other fees on imported phones: 14% VAT, 5% "development" fees, 5% airport fees, and 5% regulator (NTRA) fees. In March 2022, Egypt went a step further and barred the importation of mobile phones altogether. With a view to controlling foreign exchange flows, Egypt prohibited 13 items (including phones) from being imported into the country without prior Central Bank approval; no such approval has since been granted for the import of phones, resulting in an effective ban on imports. These import barriers frustrate and contradict the government of Egypt's stated digitalization goals, as mobile phones are a critical catalyst for digital transformation. The measures also give fodder to illicit trade in products, as this becomes the only channel through which mobile devices can be imported into the country.

Recommendation: The Government of Egypt should adhere to its WTO commitments and remove tariffs and other barriers to the import of mobile phones.

EUROPEAN UNION

European Union Cloud Cybersecurity Scheme (EUCS) Excludes U.S. Cloud Services Providers:

The EUCS excludes U.S. providers of cloud services by making local ownership and control the deciding factor in assessing whether a cloud service provider can be deemed as meeting the highest level of cybersecurity. This measure is expected to become mandatory, and could be expanded to apply to E.U. private sector industries deemed "essential," including banking and financial services, energy, healthcare and transportation. The EUCS builds on a previous regulatory effort in France known as SecNumCloud, discussed below, and has the potential to significantly disrupt U.S. exports of cloud services.

This approach that violates the E.U.'s WTO trade obligations, and it sets a worrying precedent by signaling that the E.U. does not consider U.S. firms to be trustworthy.

Recommendation: The European Union should drop the country-of-origin requirements in the EUCS and adopt a risk-based approach to cloud services that does not impair the ability of U.S. companies to provide cloud services to all parts of the economy.

E.U. Standards Strategy Excludes Non-EU Participants

Pursuant to the implementation of the 2022 Standards Strategy, the European Union made changes to Regulation (E.U.) No 1025/2012 and to its engagement with European Standards Organizations (ESOs), like the European Telecommunications Standards Institute, that have limited the ability of U.S. companies and other global stakeholders to participate in the development of some standards.

Openness is fundamental to the development of standards. As noted in the WTO TBT principles regarding standardization, "Membership of an international standardizing body should be open on a non-discriminatory basis to relevant bodies of at least all WTO Members. This would include openness without discrimination with respect to the participation at the policy development level and at every stage of standards development."

As Europe continues to use standards to confer regulatory compliance – itself a concerning deviation from the WTO's emphasis on the voluntary nature of standards – the ability of U.S. companies to fully participate in the development of standards will only become more important.

Recommendation: The European Union should retract the measures excluding global participants from fully participating in all standards activity.

Carbon Border Adjustment Mechanism

The Carbon Border Adjustment Mechanism ("CBAM") imposes a requirement on businesses to report on embedded emissions of imports. In January 2026, CBAM will also add a carbon price on imports in emission-intensive sectors (cement, iron, steel, aluminum, fertilizers and electricity) whose production/related emissions have not been taxed (or not at the same level as the EU) in the producer's country. This is important to ICT companies – because these companies use some of these components in ICT products. Additionally, businesses will have to purchase and surrender "CBAM Certificates."

Even for small imports, CBAM imposes a significant compliance burden. The first year of reporting created uncertainty as U.S. suppliers were forced to grapple with a lack of clear guidance, available tools, and time and resources invested in compliance. The next steps of the CBAM implementation will

further raise costs for importers in Europe since free Emissions Trading Scheme ("ETS") allowances will be gradually phased out.

CBAM discriminates against products from countries like the United States that do not have equivalent carbon emissions taxation schemes in place.

Recommendation: The EU should look to harmonize its CBAM requirements to avoid costly compliance burdens for importing ICT products from the U.S.

Deforestation Regulation

The EU's Regulation on deforestation-free products ("EUDR") creates a due diligence process for companies regarding the import of deforestation-risk products such as palm oil, timber, cocoa, coffee, leather, wood, pulp and furniture, among others. U.S. companies market collaboration suites that include wood furniture and other pulp/wood fiber products.

Pursuant to the EUDR, businesses must provide a statement demonstrating compliance with all relevant local laws in each exporting country along with full traceability of the goods throughout their supply chains. The regulation also provides for periodic reviews that would expand the regulation's scope to cover new products and ecosystems. Information requirements include geolocation data to the exact plot of land where the covered material was produced and documentation demonstrating that there has been no deforestation or degradation of forest in the relevant area since December 2020.

EUDR is imposes significant compliance costs and creates conflicting legal requirements due to its extraterritorial application (*i.e.*, imposing compliance obligations on suppliers in third countries). The EUDR also makes sourcing raw material more challenging due to current and potential third country suppliers' inability and lack of capacity to comply with the regulation. While the EU keeps postponing the entry into force of the EUDR, a substantial review of the rules or the removal of the law as such is critical.

Recommendation: TIA urges the EU to conduct a review of the EUDR and its substantial compliance costs which could create a barrier of entry to the EU for many in the ICT industry. The EUDR should also avoid any extraterritorial compliance requirements, forcing importing companies to shoulder the burden of ensuring compliance for third-party suppliers in different jurisdictions.

Data Act Article 32 on International Government Access and Transfer

The EU Data Act establishes rules and "safeguards" for foreign governmental bodies' access requests to non-personal data stored in the EU. Specifically, Article 32 of the EU Data Act (2023/2854) provides that data processing services "shall take all adequate technical, organizational and legal measures, including contracts, in order to prevent international and third-country governmental access and transfer of non-personal data held in the Union where such transfer or access would create a conflict with Union law or with the national law of the relevant Member State."

Article 32 of the Data Act makes U.S. companies responsible for potential conflicts in law relating to governmental access to data. At a minimum, this de facto item requires companies to conduct and publish evaluations of U.S. and other non-EU laws equivalent to the Transfer Impact Assessments (TIA)

under the General Data Protection Regulation (GDPR) for non-personal data, which is disproportionate to the risk presented. GDPR TIAs are already very complex for U.S. companies providing data processing services for *personal* data. In a maximalist scenario, it could force U.S. companies to localize nonpersonal data infrastructure and operations to provide the requisite guarantees. This measure is specifically targeted at and discriminates against U.S. companies due to EU concerns around U.S. governmental authorities' requests for information.

Recommendation: We urge the EU to substantially review the requirements of the EU Data Act and harmonize them with laws of the EU's trading partners, including the U.S., so that they do not specifically target the way U.S. companies store and process their data in compliance with U.S. law.

EU Preference in Public Procurement and Funding Instruments

Since taking office in December 2024, the new European Commission has repeatedly supported the introduction of European preference criteria in EU public procurement and funding procedures. The reform proposals are due to be published in 2026 and raise concerns amongst U.S. businesses with operations in Europe.

The European Commission plans to launch a comprehensive public procurement reform in 2026. As part of the reform, the Commission plans to propose European preference criteria for strategic sectors. Similarly, the recent Defense EDIP/SAFE proposals and the Clean Industrial Deal reference EU content requirements as one of the criteria and a mandate for funding. We expect the upcoming Industrial Decarbonisation Act (IDA) and Cloud and AI Development Act (CAIDA) to include similar requirements. The strategic sectors under scope are yet to be defined but could include clean energy technologies, along with critical technologies that are deemed important for Europe's industrial and economic security, such as AI, quantum, and advanced semiconductors.

The EU's proposed European preference is discriminatory and contrary to the EU's international trade obligations, which incorporates a principle of non-discrimination and requires that treatment accorded to the goods and services of other GPA Parties shall be no less favorable than the treatment accorded to domestic goods and services. European preference criteria and EU content requirements will limit U.S. businesses' ability to access parts of the EU government procurement market, impacting a wide range of industrial sectors including defense, clean tech and critical digital technologies.

In addition, the EU is also progressively adding localization requirements in new Research and Innovation projects (eg, under Horizon 2020), notably those related to 6G and secure connectivity projects, excluding U.S. companies from the initiatives.

Recommendations: As the EU proceeds towards procurement reform next year, it should remove discriminatory barriers for companies in trusted allied jurisdictions, such as the U.S., in order to be more aligned with the realities of the global ICT sector.

FRANCE

SecNumCloud is a national cybersecurity certification scheme for cloud service offerings that handle sensitive data, primarily in the French public sector.

France's SecNumCloud is an burdensome trade practice and barrier to market access, because it requires cloud providers to store data, and conduct primary operation and supervision, in the EU and guarantee protection against extra-European legislation, such as the U.S. Cloud Act. In addition, certified

cloud providers must be headquartered in the EU, and their ownership must be under European control to be eligible to supply covered cloud services. As a result, U.S. companies do not qualify to supply cloud services to specific French government procurements for sensitive data, including in the healthcare and defense sectors.

France is expected to extend the SecNumCloud certification requirement to "Operators of Vital Importance" (OVI), such as banks, energy, and telecommunications providers, a move that would further limit market access for U.S. cloud service providers.

Recommendations: TIA urges France to remove requirements for cloud service providers to be located in the EU and harmonize the SecNumCloud to be in line with other global cyber certification efforts.

INDIA

The issue of greatest concern to TIA in India is New Delhi's repeated imposition of import duties on ICT products, in violation of its WTO obligations.

When India joined the Information Technology Agreement in 1996, it agreed to grant zero-duty treatment to many ICT goods, including telecom equipment products classified under the 8517 harmonized system (H.S.) heading. In 1997 the Indian government modified its GATT schedule to reflect those changes, and under a staging process, introduced a plan to eliminate duties on all 8517 products by 2005. In accord with its WTO obligations, in 2005 India formally updated domestic customs regulations to provide for zero-duty rates on the goods.

However, in a clear breach of those commitments, India has subsequently levied duties on covered products on seven separate occasions. These actions violate the basic WTO obligations on duty treatment documented in India's GATT schedule.

A brief chronology follows:

- In July 2014, India rescinded a duty exemption and implemented a 10 percent basic duty on a range of advanced telecom technologies classified under the 8517 heading.[1]

- Three years later in July 2017, New Delhi again imposed import duties of 10 percent, this time on a much broader group of telecom equipment products including mobile phones, smart phones, and base stations.[2]

- Only five months later in December 2017, India boosted the duty rate on cell phones and smart phones once more, from 10 percent to 15 percent.[3]

- In February 2018, India further increased the duty on cellular mobile phones from 15 percent to 20 percent, while raising duties on phone parts from a range of 7.5-10 percent to 15 percent. The duty on wearable devices was raised from 10 percent to 20 percent.[4]

- In April 2018, India announced it will impose a 10 percent duty on populated printed circuit boards (PCBs) used in mobile phones.[5]

- In October 2018, India said it will double the 10 percent levy on telecom goods including base stations, smart watches, optical transport and VOIP equipment to 20 percent[6] and impose a new 10 percent duty on parts and components of telecom products[7] that were previously not subject to duties.

- In February of 2020, India's Union Budget proposed increasing customs duties on mobile phones and mobile phone components including fingerprint scanners, printed circuit board assemblies, by 10%.

- In February of 2021, India's Union Budget again proposed increasing customs duties on mobile phone components including camera modules, connectors, printed circuit board assemblies, parts for the manufacture of lithium ion battery packs, and mobile phone charger inputs. These duties were put into place on February 2 pursuant to Customs Notification 03/2021.

- In 2024, India's budget proposed decreasing customs duties on mobile phone, printed circuit board assemblies ("PCBAs") for mobile phones, and chargers to 15%; while at the same time increasing duties on PCBAs for specified telecommunications equipment.

At the same time, New Delhi has rolled out multiple rounds of duties, it has clearly proclaimed its protectionist intentions to keep out foreign goods and create a domestic telecom equipment industry.

India's national Digital Communications Policy released in September 2018 calls openly for "rationalising taxes and levies and differential duties to incentivize local manufacturing of [digital communications] equipment, networks and devices." It also called for incentivizing private operators to buy domestic Indian telecom products. Unfortunately, India's protectionist policies have made U.S. products more expensive and less competitive in the marketplace, effectively shrinking American market access.

These tariffs specifically have led some TIA member companies to reduce U.S. manufacturing for certain products that they had previously exported to India.

***Recommendation*:** We urge the Indian government to rescind the aforementioned duties on imported ICT equipment as soon as possible. The new levies have not only hurt investor confidence, but risk needlessly raising the price of technology products and services for India's own businesses and citizens, which will make it more difficult for the government to achieve the goals of Digital India.

We also encourage USTR to take further action in the context of the WTO with the goal of getting India to comply with its tariff bound rates on ICT products.

<u>Excessive and Redundant Requirements for In-Country Tests and Certification</u>

In 2018 India introduced a sweeping system of required in-country tests and certifications for telecom equipment, MTCTE (mandatory testing and certification for telecom equipment). The policy was not initially notified to the WTO in draft form.

The requirements impose needless costs on ICT companies, which already conduct such tests in internationally accredited labs in other geographies. Testing fees may cost up to 50 lakhs rupees or

$78,000 per product when carried out by government labs, and no price cap has been established for commercial labs. The system of certifications will eventually cover all types of telecom equipment, ranging from simple IoT devices to fully functioning base stations.

While the policy was initially intended to become effective October 2018, India's Department of Telecommunications (DoT) subsequently delayed implementation. By October of 2019 the Department of Telecommunications made MTCTE mandatory for 2-wire telecom equipment, modems, G3 fax machines, ISDN CPE, private automatic branch exchange (PABX) systems, and cordless telephones. Since that time, DoT has continued to expand the requirements under "Phase II" of the plan to cover areas including Transmission Terminal Equipment, the PON family of Broadband Equipment, and feedback devices as laid out in TEC/01/2017-TC on June 23, 2020. These requirements were notified to the WTO under G/TBT/N/IND/158, G/TBT/N/IND/159, and G/TBT/N/IND/160 in August of this 2020 and became compulsory as of October 1, 2020.

India has continued to expand testing and certification requirements under "Phase III" and "Phase IV," which cover 32 products categories including: equipment operating in the 2.4 GHz and 5 GHz Bands, IoT Gateways, Local Area Network Switches, Routers, Conferencing equipment, and Base Station Control/Radio Network Controllers. While some of these requirements – such as those requirements for mobile phones and smart watches – have been delayed, it is our expectation that GOI will continue to move forward in implementing this technical barrier to trade.

In June 26, 2023 India released details regarding “Phase V” of MTCTE covering Base Station for Cellular Networks, 5G Core, Hypervisor, E-band Fixed Radio Relay Systems, Converged Multi Service Application Access Equipment, IP Terminals, and Hybrid Set Top Boxes. While the expectation had been that the certification regime for these Phase V products would come into effect by July 1, the mandatory certification deadline for these products has been delayed until January 10 for Hypervisors and IP terminals and until September 30 for 5G base stations and E-band Fixed Radio Relay Systems. MTCTE certification deadlines for Smart Electricity Meters, Satellite Communication Equipment, 4G base stations, SIM, and VHF UHF Radio Equipment Systems were also delayed in the notice from India’s Telecommunications Engineering Centre (F.No. 5-2/2024-TC/TEC).

Besides the lack of available tests for some of the prescribed parameters, India's current lab capacity for electromagnetic compatibility (EMC) and electromagnetic interference (EMI) is limited, and the number of certification bodies exist nationwide to review results and summary reports is insufficient. Because of the local requirements, this lab capacity has to support both testing for the local market and testing for ICT exports. India has permitted the use of ILAC-accredited lab reports or certain “highly specialized equipment” (HSE), which cannot be tested in the current India lab ecosystem. However, the lab report must be no older than two years, requiring re-testing of products that have not changed in the intervening two years. Allowing more flexible use of global labs could increase the capacity of U.S. manufacturers to access testing and certification services and accelerate India’s own goal to export more telecommunications products.

Moreover, there is no need for India-based tests, as global vendors already certify products to a high level of international standards in areas such as radio frequency and safety. Requirements to test once again for the Indian market will not improve safety but merely incur needless and unnecessary costs for suppliers. Telecom suppliers worry that intrusive testing could potentially allow for leaks of proprietary information.

Recommendation: TIA urges the government to indefinitely allow ICT equipment vendors use internationally accredited labs in any global location to conduct testing. Where such tests focus on security issues, India should recognize Common Criteria certifications from countries that are parties to the Common Criteria Recognition Arrangement of which India is one. To the extent that testing continues to be required, the government of India should also give companies the option to either conduct in-country testing in India or submit test reports from an accredited global test lab. This will help the government to ensure quality and safety along the various parameters will be met.

We further encourage the Indian government to reference internationally-recognized standards to be used in such testing. Such an approach allows for robust security vetting without imposing new fees that will drive up end user costs or needlessly delay time to market for ICT products.

We appreciate USTR's approach to seeking reductions in technical barriers to trade by encouraging India to accept test results from accredited conformity assessment bodies on a bilateral basis whenever possible for non-agricultural goods as stated in the January Trade Policy Forum Joint Statement. While we hope this effort yields fruit, ultimately we continue to believe India should accept test results from accredited labs regardless of the jurisdiction where that testing occurs. TIA does not support the creation of an MRA with India.

Source Code Disclosure Requirements as Part of Security Testing

As a part of its Communication Security ("COMSEC") scheme, implemented pursuant to the India Telecom Security Assurance Requirements ("ITSAR"), India's Department of Telecom requires U.S. companies to disclose valuable U.S. source code as a condition for market access.

USTR raised this issue via the U.S. Ambassador to India in January 2025. Submission of source code was originally mandated and then the Indian Government reformed the requirement via a notification in June 2025.

While the India government is no longer requiring source code submission for certification, the requirement remains written into the regulation, leaving companies to rely on the assurances of the government for the time being. The government is currently requiring OEMs to submit the following: 1/internal test report excluding IP information, including summary of security vulnerabilities / weaknesses classified by risk; and 2/ The "Self Declaration of Conformity" stating that the source code is free from specific vulnerabilities and an undertaking stating, in case of an attack due to product in question, source code will be submitted for testing.

This new requirement continues to be a challenge for many reasons. The requirement to provide source code in the event of an attack/incident still remains, and the threshold and arbitration of attack or incidence is not defined. Further, source code includes algorithms, protocols, or defense-in-depth mechanisms, all of which are export-controlled under U.S. law. Ultimately, this source code constitutes commercially valuable, confidential, and sensitive information. Divulging proprietary information to testing labs and agencies could lead to the leakage of business confidential information to the competition and endanger the privacy and security of individuals and the OEMs.

Recommendations: TIA recommends that the Indian Government revise the existing ITSAR to remove all language requiring source code disclosure. In the alternative, we urge India to drastically reform the

ITSAR requirements and ensure that security certifications are based on international standards (e.g., Common Criteria, ISO/IEC 27001/62443). Additionally, India Penetration testing and product-specific Vulnerability Assessment and Penetration Testing (VAPT) should be conducted by certified labs under agreed scopes instead of source code testing.

Preferential Market Access (PMA)

India has recently issued a series of policies to promote government purchases of locally made ICT products, including the following:

In January 2017 the Department of Telecommunications issued conditions for a list of telecom products under which they could qualify as domestic and therefore be accorded a preference in government procurement. Under the Public Procurement (Preference to Make in India) Order issued in June 2017 by the Department of Industrial Policy and Promotion, government agencies and companies are requested to accord a 20% price preference to products containing more than 50% local content. In September 2017, the Ministry of Electronics and Information Technology issued a lengthy list of cybersecurity products that will be subject to this order. The agency subsequently updated and re-iterated these requirements in procurement orders issued in 2018, 2019, and 2021.

At a practical level, local content requirements are often difficult to meet. For example, the procurement preference for 50 percent local content is difficult to meet for many switching systems used in telecommunications as well as satellite systems. It is not currently possible to manufacture such systems in India while meeting the necessary technical requirements outlined in tenders.

Like all countries that manufacture ICT products, India's ICT manufacturing base depends on a globally flexible supply chain that is characterized by intense competition and fluctuations in price and supply of different inputs. Market demands are such that it would be impractical for the commercial sector to eliminate the use of global resources or a distributed supply chain model.

Recommendation: Since India is not currently a member of the WTO Government Procurement Agreement (GPA), we acknowledge that this policy is not in conflict with its formal agreements. However, we would submit that the PMA policy does a disservice to the Indian government in limiting access to the most cost-effective and advanced ICT products available, especially at a time when officials are implementing important new programs to promote digital connectivity nationwide. We would urge the Indian government to consider a procurement policy that grants agencies maximum flexibility, allowing them to purchase products based on performance, operational needs, and overall cost, rather than focusing on local content requirements.

Local content mandates have not historically proven effective in promoting the development of local products that are either high quality or cost competitive. Instead of granting domestic preferences in public procurement, a better way to help local industry would be to focus on enhancing the business environment to foster healthy competition and encourage innovation.

As the Indian government seeks to enhance exports, we would encourage it to take a closer look at the practices reflected in the GPA and consider how they might bring their practices into alignment with it. Ultimately, joining the GPA would expand the access of Indian's own I.T. industries, including its services sector, to government procurement markets around the world.

Freedom to Use Strong Encryption

TIA urges India to adopt policies allowing the use of strong encryption algorithms that have been reviewed by international experts for robustness and security assurance to protect corporate and personal information online. The freedom to use strong encryption is a global standard for securing information online, such as confidential business information, financial information, online transactions, and internal government communications, from intrusion by hackers, thieves, competitors, and other wrongdoers.

Recommendation: TIA urges the government of India to amend its current encryption policy to allow for more robust encryption, which will enable India's rapidly growing I.T. enabled services and business process outsourcing industries that rely on strong encryption to secure their global clients' confidential information. India should adopt policies that protect the freedom to use strong encryption online and, consistent with global practice, not limit the type of encryption technologies that can be employed by the private sector.

Duplicative Security Certification Schemes Being Promoted by the Indian Government

In July 2019, India's Ministry of Electronics and Information Technology (MeitY) released a duplicative security certification known as the "Trusted Electronics Value Chain – Compliance Scheme" (TEVCCS). TEVCCS is technically equivalent to IEC/ISO 20243 -1 & 2 (Information Technology - Open Trusted Technology Provider Standard or OTTPS) but stipulates certification by MeitY's Standardisation, Testing and Quality Certification (STQC) Directorate. The draft scheme envisages certifying the processes that apply to commercial, off-the-shelf ICT hardware and software throughout the entire product life cycle encompassing the areas of technology development and supply chain. Currently, the certification scheme is voluntary, but there are significant indications that it may be converted to a mandatory certification requirement. This new requirement will add to the long list of existing certification schemes in India and potentially subject confidential elements of product design and supply chain to additional government audits.

Recommendation*:* We request that MeitY avoid formally or informally mandating the use of the TEVCCS.

Delays in Wireless Planning Commission (WPC) Certifications

Imports of certain electronics and ICT products require certification from the Bureau of Indian Standards (BIS) and "equipment type approval" from the Wireless Planning & Coordination wing of the Ministry of Communications. The procedure for obtaining these approvals is massively time consuming and opaque, with undefined timelines that often produce inordinate delays. The lack of transparency, predictability, and timeliness creates a significant barrier to imports.

Recommendation: We request that the Indian government expedite the process to reduce the processing time and make it process more transparent.

F.M. Radio Receiver Advisory Raises Concerns

On April 28 of 2023, MEITY circulated an advisory stating that handset manufacturers should build F.M. radio receiver functionality into mobile phones. Because of the tightly integrated design of mobile phones, a requirement to do so would require a significant redesign of many handsets currently available on the market and would constitute a technical barrier to trade.

Recommendation: The Government of India should refrain from making F.M. radio a mandatory requirement.

TRAI Proposal to Ban Permanent Roaming for IoT Devices

In March of 2024, the Telecom Regulatory Authority of India (TRAI) released Recommendations on Usage of Embedded SIM for Machine-to-Machine (M2M) Communications, which included a provision that would ban permanent roaming for any M2M eSIM fitted in imported devices and require those devices to be reconfigured into local communications profiles within six months. If adopted, this recommendation would limit the ability of U.S. companies to sell products in the Indian market, as well as ultimately raising costs for companies and raising prices for consumers.

Recommendation: The Government of India should reject the TRAI recommendation.

INDONESIA

Protectionist Policies including Local Content Requirements

We are concerned about a pattern of Indonesian regulations issued in recent years that provide a framework for protectionist measures, some of which target ICT goods and services. In 2014, the Indonesian government finalized a trade bill that authorizes the government to take protectionist steps such as restricting exports and imports with the goal of helping local industries.

In 2015, the Ministry of Communications and Information Technology issued regulation no. 27, which imposes local content requirements on LTE-based telecom equipment that would rise to 40% for base stations and 30% for subscriber stations within two years of the date of implementation. This follows the ministry's earlier issuance of two decrees, a wireless broadband decree in 2009 and a telecommunications decree in 2011, that place restrictive local content requirements and sourcing requirements on service providers. The "wireless broadband decree" requires local content of 30 to 50 percent in the wireless broadband sector. The "telecommunications decree" requires all service operators to spend 35 percent of their capital expenditures on domestically manufactured equipment.

Currently, at least 40 percent of the equipment must be locally sourced, but within the next five years it is expected to increase to 50 percent. These provisions are reiterated in Article 6 of the 2011 decree on the use of the 2.3 GHz Radio Frequency Band (19/PER/M.KOMINFO/09/2011

In 2016, the Communication and Information Technology Ministry proposed new regulations that would require foreign companies that provide online content to set up formal offices in Indonesia according to national tax law and abide by a number of other requirements, including local censorship rules. The high costs of complying with such a mandate could make it difficult for many smaller foreign service providers to operate in Indonesia, and as a result, may limit Indonesian access to innovative online applications that would be available in other global markets.

Finally, Ministry of Industry Regulation No. 22 of 2020 concerning Terms and Procedures for Calculating the Value of Domestic Component Level for Electronic and Telematics Products set out a 70%

requirement for the manufacture of digital products. Although it is unclear whether the government has achieved this target, recent ban on imports of ICT goods suggests that this policy will continue to place an additional administrative burden on the production of physical ICT products that are indispensable for ICT companies to operate in Indonesia. Such onerous requirements cannot be met without vendors establishing a manufacturing presence in Indonesia.

Recommendation: TIA urges the government of Indonesia to rescind local content requirements that limit technology choices available to its consumers and businesses.

Data Localization

Regulation No. 82 of 2012 requires operators of "public services" to locate data centers on Indonesian territory. This was modified in Government Regulation No. 71 of 2019, but it remains a barrier to trade.

Recommendation: Data localization is likely to impede innovation by rendering international communication more difficult; moreover, by increasing costs, the regulation threatens to discourage service providers from entering the Indonesian market. Rescinding the data localization requirement would serve to promote investment by alleviating investor concerns over the expense and time associated with compliance.

Classification of Zero-Duty Digital Goods in Tariff Schedule

In February 2018, the Indonesian Ministry of Finance issued regulation No. 17, which established five eight-digit tariff lines under chapter 99 on software and other digital products. Though initial duty rates were established at zero, the treatment of services as potentially dutiable goods creates a worrying precedent. Any imposition of duties on such goods would appear to violate the WTO's moratorium on e-commerce, in which members agree to abstain from imposing duties on electronic transmissions.

Foreshadowing this development, at the MC11 trade ministerial in Buenos Aires in 2017, Indonesia circulated a communication saying it is Jakarta's understanding that the e-commerce moratorium "applies only to the electronic transmissions and not to products or contents which are submitted electronically." In practice, such an approach is at odds with the moratorium and would render it effectively meaningless. While Indonesia has since indicated its intention to support the WTO Moratorium, though it remains to be seen if Indonesia will indeed do so. However, Indonesia has not yet removed rules under Ministry of Finance Regulation 26/2022 that established import categories for software downloads and digital products under Chapter 99 of its tariff schedule (and provide assurance that the digital products would remain duty-free) as well as Ministry of Finance Regulation No. 190/PMK.04/2022 that established a new import declaration procedure for intangible goods, which had paved the way for Indonesia to administer and collect duties on digital products should Indonesia decide to impose unilateral tariffs on digital products and electronic transmissions.

Recommendation: We urge the Indonesian government to remove digital services it has pledged to keep duty-free from its tariff schedule.

Assessing Customs Duties in Excess of its Bound Rates

Since 2018, Indonesia has been assessing customs duties on ICT products that are in excess its obligations under its WTO Goods Schedule. For example, certain routing and switching products under

HTS Code 8517.62 are being assessed a 10% duty, when Indonesia has committed to provide duty-free treatment in its Good Schedule.

Recommendation: The Government of Indonesia should restore duty-free treatment to products that are bound at zero under Indonesia's WTO Goods Schedule.

MALAYSIA

Import Certification

Malaysia requires importers to obtain a certificate of approval issued by the Standard and Industrial Research Institute of Malaysia ("SIRIM") to import communications equipment. However, SIRIM does not undertake testing of refurbished products as import of refurbished equipment is prohibited in Malayasia. This ban on refurbished products limits U.S. suppliers' ability to support customers in Malaysia. For products still in production, new components must be sourced to support customers. For products that are no longer in production, such products cannot be supported or replaced with available refurbished parts, meaning that U.S. suppliers are forced to stop customer support or the customer is forced to upgrade to a newer version of the product.

Additionally, SIRIM requires Internet Protocol Version 6 ("IPv6") certification at the level of "IPv6 Ready Logo" for all products imported into Malaysia. While the "IPv6 Ready Logo" is a voluntary certification led by the IPv6 Forum, the certification is mandated in Malaysia. This requirement is is out of synch with a similar requirement in the U.S. because the US requirement only applies to government procurement, rather than general market entry. Malaysia's unique practice of specifically requiring Malaysia IPv6 compliance for market entry is excessively burdensome and out-of-step with other countries' practices.

Recommendations: TIA urges Malaysia to harmonize their requirement of the IPv6 Ready Logo with other countries, and revise their ban on refurbished products so U.S. companies can continue to service Malaysian customers using legacy products with refurbished parts.

MEXICO

Local SAR Testing Requirements

In February of 2020, Mexico's Instituto Federal de Telecomunicaciones (IFT) published new guidelines pursuant to Technical Provision IFT-012-2019 that pose a significant barrier to trade for mobile telecommunications products. These guidelines came into effect in February of 2021, and they restrict sales from U.S. companies and delay time to market by requiring in-country testing for Specific Absorption Rates (SAR). These testing requirements are not only redundant and have no conceivable benefit to Mexican consumer safety, but also they also refer to out-of-date standards instead of recent guidance from the IEC/IEEE and ICNIRP. These requirements also lack the normal clauses exempting retroactive compliance, raising the specter that not only would new products require testing but also all existing products would require testing. Finally, these testing requirements would seem to indicate a breach of Mexico's commitment to national treatment for conformity assessment bodies pursuant to Article 11.6 of the USMCA.

Currently, there are only a few accredited laboratories for SAR testing, which creates bottlenecks for testing new products and may cause time-to-market delays. Industry has repeatedly asked the IFT to accept interim certificates and/or international test reports until the testing laboratory infrastructure is sufficiently established and robust in the country.

Recommendation: We recommend that the Government of Mexico (GOM) eliminate these duplicative and unnecessary domestic testing requirements. TIA also recommends that the U.S. government push Mexico to engage further on this issue in the context of ongoing USMCA implementation discussions with the goal of having Mexico accept test results from U.S. accredited labs, possibly through the inclusion of SAR testing in the U.S.-Mexico telecom MRA.

Capricious Government Procurement Practices Violating USMCA Obligations

Mexico has violated its USMCA commitments related to government procurement. For example, while implementing its "Internet Para Todos" project in mid-2020, a subsidiary of the Comisión Federal de Electricidad (CFE) issued Requests for Information for telecommunications products seemingly with the express goal of having these contracts go to Huawei Technologies. In issuing RFIs pursuant to this initiative, CFE neglected to publish public notices, named and/or described Huawei products instead of creating vendor neutral criteria, and left a period of only days between the release of the RFI and the eventual selection of a vendor. This would seemingly violate several articles of Chapter 13 of the USMCA on government procurement, and it illustrates broader industry concerns about non-transparent government procurement practices in Mexico.

Recommendation: We recommend that the Government of Mexico stringently implement government procurement practices in line with its commitments under USMCA Chapter 13.

New Labeling Requirements Violate USMCA Telecom Annex Provisions

On August 4 of 2023, Mexico's IFT put out new draft guidelines regarding the labeling of telecommunications products that would require the use of physical NOM labels on telecommunications decides.

If implemented, this requirement would violate Mexico's commitments under Chapter 12.C.4 of the USMCA. In this sectoral annex, parties to the agreement commit that, "if a Party requires equipment subject to electromagnetic compatibility and radio frequency requirements to include a label containing compliance information about the equipment, it shall permit this information to be provided through an electronic label."

Recommendation: IFT should allow the use of e-labels for telecommunications devices in line with its commitments under Chapter 12 of the USMCA. As appropriate, USTR should work with the FCC and other agencies to support Mexico's compliance with the agreement via an exchange of technical information regarding the use of e-labels.

Spectrum Allocation Policies that Favor Domestic Incumbents

Mexico maintains a method for pricing spectrum that supports large, domestic incumbents at the expense of U.S. companies that provide – or seek to provide – telecommunications services in the country. By dissuading competition, Mexico may be in violation of its Chapter 18 obligations in which

parties commit that they "shall endeavor to rely on an open and transparent process that considers the public interest, including the promotion of competition."

Recommendation: The Mexican government should adjust its method for assessing spectrum fees and adjust spectrum valuation to include factors like coverage commitments. This would promote competition and ultimately lead to more benefits for Mexican consumers.

SOUTH KOREA

Cloud Security Assurance Program for Government Procurement

South Korea's Cloud Security Assurance Program ("CSAP") provides stringent certification requirements for foreign CSPs. The regulation directs CSPs to create Korea specific products to sell to Korean central, local, and provincial agencies and public sector institutions.

In 2023, South Korea amended the CSAP and established a three-tier classification of the public institution data systems based on risk levels. Under the amended CSAP, CSPs must meet physical data segregation requirements to obtain the medium and high-risk tier certifications. This measure is a barrier to trade because foreign cloud service providers and cloud-based services cannot meet these Korea-specific requirements.

Recommendation: Revise the CSAP to remove the requirement for global ICT manufacturers to make Korea-specific products in order to enter the procurement market.

TAIWAN

In-Country Testing Requirements

Since 2021, Taiwan's National Communications Commission ("NCC") has mandated firewalls, switches, and routers deployed in critical telecommunications infrastructure to undergo re-certification at two designated laboratories located in Taiwan, regardless of any existing certifications from foreign laboratories (e.g., U.S.-based laboratories that are already recognized by the Taiwan government). The local testing in the two designated testing facilities – one of which is affiliated with the Ministry of Digital Affairs ("MODA") and the other a private laboratory named "Onward Security" – are mandatory under MODA regulations. Furthermore, each firmware update requires additional re-certification in both Taiwanese laboratories.

Taiwan's Bureau of Standards, Metrology and Inspection ("BSMI") regulates safety, health, and environmental standards for imported products. Under its recent draft regulation on "Relevant Inspection Regulations for Information Products, Audiovisual Equipment, and Ten Other Categories of Goods Subject to Mandatory Inspection", BSMI has proposed new requirements that would require U.S. companies to re-certify products and rely on local laboratories for cybersecurity testing. These duplicative rules would significantly increase compliance costs, delay time-to-market, and create unnecessary barriers for U.S. exporters.

Such dual certification requirements, coupled with the mandatory re-testing of firmware updates, creates significant trade barriers by requiring redundant and unnecessary testing. U.S. companies already invest heavily to meet internationally recognized standards, and BSMI should accept

certifications from accredited global testing laboratories instead of mandating re-testing in Taiwan. Unless addressed, these measures risk discouraging investment and limiting the competitiveness of U.S. technology products in Taiwan's market.

Recommendation: TIA urges the NCC to revise their in-country testing requirements to accept testing from laboratories that are already recognized by the Taiwan government. Additionally, BSMI should not adopt their proposed in-country cybersecurity testing requirements.

VIETNAM

Import / Export License Requirements for Encrypted ICT Products

Vietnam's Government Cipher Committee ("GCC") requires that the import and export of any product containing cryptographic functionality obtain specific permits and licenses. Suppliers importing and exporting IT products with regulated data encryption capabilities (civil cryptography products or "CCP") must obtain a Cryptography Trading License ("CTL") and a Cryptography Import License ("CIL").

These requirements add a significant burden on importing because it takes several months to obtain CTLs and CILs. Detailed information needs to be submitted alongside the application, including detailed product information, defined technical plans, information regarding the equipment's cryptographic functions, information regarding local personnel, and other material. In seeking to meet these requirements, companies often experience delays and inconsistent/non-transparent approvals or rejections by the GCC. These burdensome requirements, and the routine follow ups that the GCC requires, limit the ability of companies that invest in Vietnam to import critical hardware. A new regulation for cryptographic certification equipment, the Circular 23/2022/TT-BQP of Ministry of Defense, has introduced further uncertainty.

In addition to the license required for CCP, since April 2024, Vietnam introduced an additional cyber information security licensing requirement for products designed with functions to maintain cyber information security. As such, products previously determined to be exempted from the CCP licensing now require a separate license from the Ministry of Information and Communication. The application process and required documentation are unclear, and many company's initial applications for cyber information security trading license still remain pending approval. The dissolution of the Ministry of Information and Communication in February 2025 further adds to the confusion, as it is unclear if the license authority would be transferred to the Ministry of Public Safety or to the Ministry of Science and Technology. The vacuum of regulatory authority also creates uncertainty about how to obtain the necessary licenses to continue import to Vietnam.

Recommendations: TIA urges the Vietnamese government to issue regulatory clarity on necessary licenses for importing into the country, and to work with the ICT industry to ensure those licenses are streamlined and efficient as possible so as not to increase costs to importing companies and Vietnamese citizens.

Prohibition on the Import of Refurbished Products

Vietnam maintains import prohibitions on certain used information technology ("IT") products. While Decision 18/2016/QD-TTg eases import prohibitions on some used IT products, lenient treatment only applies provided that they meet various mandatory technical regulations and standards.

This policy creates a burden on companies and consumers alike because refurbished products are "like" products to new, so prohibiting their import violates Vietnam's international trade commitments. Products and components are essential in order to continue supporting customer with products that are under warranty, especially when such products have reached end-of-sale and components are no longer available as new products. In particular, critical infrastructure customers are unable to obtain replacement parts to service and maintain critical elements of their infrastructure without access to refurbished products.

Recommendation: The Vietnamese government should revise their prohibitions on the importation of refurbished products so U.S. companies can continue to service Vietnamese customers using legacy products with refurbished parts.

DIGITAL TRADE

TIA members rely on robust protections for digital trade to drive global sales, invest in innovation, and support growing wages for thousands of workers in the United States in roles from manufacturing and deployment to R&D and customer engagement. This reliance on strong digital trade centers around three basic fact patterns:

1. **Telecommunications connect people across borders.** As a result, innovative ICT companies need to be able to sell products and services – both digital and physical – to parties around the world. These products power crossborder data flows and therefore rely on an international regime that enables, not retards, their continued growth.
2. **Manufacturers rely on a complex web of tangible and intangible inputs in production.** Unlike some commodities, the value in an ICT device is not simply derived from its physical characteristics. Rather, in many cases the value is derived in large part from software and other intangible sources of value that are transmitted digitally.
3. **The ICT sector is a global industry.** While the United States is a large market, it is dwarfed by the global telecommunications market where there are still more than 3.7 billion people who do not have access to the internet.[1]

For this reason – and more broadly because of America's competitive advantage in terms of digital products and services – the United States has for decades supported robust digital trade provisions in international agreements. These include prohibitions against the following:

- Data localization
- Restrictions on cross-border flows of information
- Forced disclosure of source code
- Discrimination against foreign digital products

The decision by political leadership inside the prior administration's office of the United States Trade Representative to turn its back on these core principles in 2023, without meaningfully consulting Congress and the broader stakeholder community, has done significant damage to the global regime that supports U.S. digital exports. This also has specific relevance to the NTE report process, which last

[1] World Economic Forum, *Coronavirus Has Exposed the Digital Divide Like Never Before* (April 22, 2020) https://www.weforum.org/agenda/2020/04/coronavirus-covid-19-pandemic-digital-divide-internet-data-broadbandmobbile/

year diverged from its statutory purpose[2] and stopped listing several digital trade barriers impacting U.S. companies.[3]

This administration has an opportunity to correct this error. TIA urges USTR to meaningfully include digital trade issues in this year's NTE. More broadly, TIA urges USTR to change course from prior disastrous reversal on digital trade issues; which harms U.S. ICT workers and shifts our digital trade policy away from global democracies and toward countries like China and Russia. Setting aside the concerns raised by the business community, there is broad support for a return to free and open internet principles across political parties[4] and among the broader stakeholder community supporting global civil liberties.[5] A full accounting of digital trade barriers in the NTE could be the first step in a more consultative process wherein USTR engages with Congress, civil liberties groups, workers organizations, and the business community to ensure that the Administration's concerns regarding the evolving nature of digital trade are more fully addressed.

[2] Pub. L. No. 93-618, § 181 requires USTR to "identity [sic] and analyze acts, policies, or practices of each foreign country which constitute significant barriers to, or distortions of—(i) United States exports of goods or services (including agricultural commodities; and property protected by trademarks, patents, and copyrights exported or licensed by United States persons), (ii) foreign direct investment by United States persons, especially if such investment has implications for trade in goods or services, and (iii) United States electronic commerce."

[3] William Reinsch, *Moving from Missed Opportunities to Actual Harm*, Center for Strategic and International Studies (April 1, 2024) https://www.csis.org/analysis/moving-missed-opportunities-actual-harm

[4] See Ron Wyden, Mike Crapo, Thomas Carper, et al., *Letter to the President of the United States on WTO Digital Trade Negotiations* (Nov. 30, 2023) https://www.finance.senate.gov/imo/media/doc/20231130wydencrapolettertopotusonwtodigitaltradenegotiations.pdf.

[5] American Civil Liberties Union, Center for Democracy and Technology, Freedom House, et al., *Coalition Letter Urging Biden Administration to Protect Free and Open Internet*, ACLU (February 26, 2024) https://www.aclu.org/documents/coalition-letter-urging-biden-administration-to-protect-free-and-open-internet.