Before the
U.S. DEPARTMENT OF COMMERCE
Washington, DC 20230

In the Matter of	)	
	)	
Securing the Information and Communications	)	Docket No. 191119-0084
Technology and Services Supply Chain	)	RIN-0605-AA51

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association ("TIA")[1] welcomes the opportunity to comment on the rules proposed by the Department of Commerce ("Commerce") to secure the information and communications technology and services supply chain.[2] As both an advocacy organization and a standards-setting body, TIA represents hundreds of global manufacturers and vendors of information and communications technology ("ICT") equipment and services that are supplied to the owners and operators of communications networks, enabling operations across all segments of the economy. Our member companies design, produce, and sell equipment and services in countries around the world that leverage modern global supply chains, and each company has a vital stake in the outcome of Commerce's work in this proceeding.

As discussed below, TIA supports Commerce's efforts but believes that some key alterations to the proposed rules will enable Commerce to secure the supply chain more

[1] TIA is the leading trade association for the information and communications technology ("ICT") industry, representing companies that manufacture or supply the products and services used in global communications across all technology platforms. TIA represents its members on the full range of policy issues affecting the ICT industry and forges consensus on voluntary, industry-based standards.

[2] *Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 65316 (Nov. 27, 2019) ("Notice"). These comments represent the views of the TIA Public Policy Committee. While ZTE (which has been specifically identified as a prohibited supplier in other rules pertaining to supply chain security) is a member of TIA, it does not have access to the Public Policy Committee or to any of its internal communications or deliberations, and so did not influence these comments.

effectively than it could under the rules as proposed, without subjecting innovation within the ICT industry to the same degree of harm that would result from the proposal as outlined in the Notice. Specifically, TIA recommends that Commerce do the following:

- Continue to work with industry and solicit feedback on creating a version of the proposed rules that expressly recognizes the need to work in harmony with other government and industry-led efforts focused on securing the supply chain,
- Clearly define the scope of transactions subject to Commerce's jurisdiction and articulate the requisite threshold that must be met in order to trigger an investigation into an ICT transaction,
- Establish a clear and predictable process for how transactions will be evaluated with adequate and meaningful procedural protections for industry, including providing notice to any investigated party, offering that party a chance to respond prior to an enforceable decision, and establishing burdens of proof for evidence that would trigger such an investigation,
- Create a mechanism for evaluating categories of transactions that could be prohibited or excluded from the rules' scope that allows a brief period for industry comment, and
- Revise the proposed rules to allow companies an opportunity to seek anticipatory guidance in a way that reduces the potential compliance burden for the ICT industry, while also establishing safeguards to balance industry's need for certainty and flexibility to enter into productive transactions against Commerce's need to manage its resources.

TIA offers these recommendations in the spirit of working cooperatively and constructively with Commerce, consistent with its longstanding belief in the centrality of public-private partnerships to supply chain security.

DISCUSSION

I. AS THE TRADE ASSOCIATION REPRESENTING THE ICT SUPPLY CHAIN, TIA HAS ASSUMED A PROACTIVE LEADERSHIP ROLE IN PURSUING AND ADVOCATING FOR POLICIES THAT WILL SECURE THE NATION'S SUPPLY CHAIN WHILE PRESERVING INNOVATION.

TIA is not new to the issues raised by the Notice. In fact, TIA has been a leading and active voice on securing the supply chain in various arenas. Among other things, TIA submitted extensive comments in the FCC's Universal Service Fund rulemaking proceeding supporting the adoption of rules that would guard against the acquisition and use of equipment and services in

U.S. networks from suspect suppliers.[3] TIA has been involved in the public debate on the importance of trusted suppliers for 5G, as well.[4] In addition, TIA has actively supported legislation before Congress that would promote information-sharing regarding supply chain risks and fund the replacement of equipment in U.S. networks that could pose a national security threat. TIA has also been an active participant in the Department of Homeland Security's Supply Chain Risk Management Task Force since its inception,[5] and it remains active in public-private ICT sector coordinating councils focused on cybersecurity and supply chain threats. Through our active participation in these efforts, as well as input from our members who constitute the core of the industry, TIA is well equipped to advocate on behalf of sensible policies that secure the nation's supply chain.

TIA's persistent focus on and interest in supply chain security is a natural extension of the ICT industry's mission. Fundamentally, the ICT industry remains focused on delivering quality products and services to their customers. Given the demonstrated risks that can flow from a compromised supply chain, no manufacturer can attest to the quality of its products without addressing the security of their supply chain. Supply chain security is thus a subset of quality and certifying the quality of ICT products is something TIA has a strong background in through our subsidiary QuestForum's TL-9000 program, which offers levels of certification for quality for ICT products.

---

[3] *See infra* Section II(B).

[4] *See, e.g.*, David Stehlin, CEO, Telecommunications Industry Association, *Telecom Industry Must Develop Trustworthy 5G Equipment Supply Chains*, BLOOMBERG LAW, Nov. 5, 2019, *available at* https://news.bloomberglaw.com/tech-and-telecom-law/insight-telecom-industry-must-develop-trustworthy-5g-equipment-supply-chains.

[5] CISA, *Information and Communications Technology (ICT) Supply Chain Risk Management Task Force*, https://www.cisa.gov/information-and-communications-technology-ict-supply-chain-risk-management-scrm-task-force.

In short, TIA speaks on these issues from the perspective of representing the ICT supply chain, standards setting bodies, and programs that have been running for decades to ensure that ICT equipment operates at an acceptable level of quality and security. It is this unique and well-informed perspective that TIA aims to bring to the issues presented in the Notice.

II. TIA SUPPORTS THE COMMERCE DEPARTMENT'S OVERALL APPROACH BUT URGES IT TO WORK WITH INDUSTRY AND GOVERNMENT PARTNERS TO REFINE THE RULES IN ORDER TO PROVIDE CLEAR DEFINITIONS AND SOUND PROCESSES TO ENABLE NARROWLY TARGETED ACTIONS.

TIA supports the inclusive approach employed by Commerce to develop this foundational regime for protecting the security of the supply chain. Commerce should maintain this collaborative posture throughout its implementation of Executive Order 13873 – during its formulation of procedural rules and continuing into its activities pursuant to the eventual final rules – in order to best leverage relevant expertise in a manner that does not conflict with or otherwise undermine other equally important supply chain initiatives taking place within industry or under the purview of other government actors.

A. TIA Supports Commerce's Decision to Seek Industry Input Before Releasing Enforceable Rules.

The Notice appears to contemplate an ongoing role for industry in Commerce's supply chain efforts, even beyond this initial request for comment. TIA applauds Commerce's recognition of the value that industry will bring to the process. Supply chain security is one of the most important and complex challenges facing the ICT industry, and industry has responded with a robust and multi-faceted effort to understand and mitigate supply chain security risks – both on its own and in partnership with government. Among other initiatives, TIA supports standards-based efforts for industry and government to collaborate on improvements to supply chain transparency, interoperability, innovation, and trust. These include TIA's own standards

and quality assurance activities focused on mitigating risks present in the ICT supply chain, as well as ongoing activities such as the O-RAN Alliance,[6] and the Telecom Infra Project's OpenRAN project group.[7]

That said, the proposed rules represent the government's first assertion of a general authority to regulate the purely private commercial ICT supply chain. This is a foundational proceeding without precedent, with the potential for significant long-term implications throughout the ICT industry. Accordingly, Commerce was correct to release its Notice asking for industry input on proposed rules prior to releasing interim final or final rules that would have been enforceable from the outset. Commerce should pursue the same industry-oriented approach as it continues to develop and adopt a framework in this proceeding. In particular, TIA urges Commerce to work with industry to refine its proposed framework in order to provide clarity of definitions and sound processes to enable narrow, targeted actions, as discussed in Section III below.

B. TIA Supports a Whole-of-Government Approach to Supply Chain Security, and the Rules Ultimately Adopted by Commerce Should Be Coordinated Closely – and Must Not Conflict – With Other Related Agency Actions.

Commerce is properly acting within its assigned responsibilities by promulgating rules that establish a process to further implement the directives of Executive Order 13873. At the same time, the proposed rules reflect Commerce's recognition that it does not enjoy an exclusive mandate over these matters. In particular, TIA commends the inclusion of Section 7.101, which does not merely permit but explicitly *requires* the Secretary to consult with the FCC Chairman, the DHS Secretary, and other heads of agency in connection with transaction reviews.

---

[6] O-RAN Alliance, *Operating Defined Next Generation RAN Architecture and Interfaces*, https://www.o-ran.org/.

[7] Telecom Infra Project, OpenRAN, https://telecominfraproject.com/openran/.

Commerce should take this obligation seriously and work in close concert with its government partners to ensure that its final rules provide for meaningful, substantive, and reliable collaboration between and among different agencies, so that no relevant expertise, proceeding, or policy interest within the broader government is overlooked.

Of course, the relevance and influence of other government actors is not limited to their potential participation in Commerce's proposed investigation process. Beyond the express call for coordination in the proposed rules, Commerce's actions must account for the fact that it is not acting alone or in a regulatory vacuum in this proceeding, and that there are numerous ongoing (and probably future) government proceedings that will inform – and be informed by – how Commerce exercises its authority under the Executive Order and implementing rules.

In particular, Commerce's exercise of its regulatory authority here will necessarily have mutually interrelated effects with other government activities now underway, namely the following:

- *FCC USF/Supply Chain Proceeding.* The FCC has adopted rules that just became effective on January 3, 2020, which among other things prospectively prohibit the use of Universal Service Fund ("USF") support on equipment and services supplied by covered entities and preliminarily designate Huawei and ZTE as such covered entities. The FCC is seeking comment on whether to expand this prohibition in time (reaching back retroactively to equipment and services from Huawei and ZTE) and in scope (applying the prohibition to covered equipment and services purchase with funds other than USF). The record being developed in that proceeding (with formal comment deadlines coming just weeks after the deadline in this proceeding), and the FCC's ultimate decisions in response to it, can and should help to guide Commerce's own actions here.

- *NDAA Section 889.* As of August 13, 2019, Section 889 of the John S. McCain National Defense Authorization Act of 2019 ("NDAA") prohibited the procurement of equipment or services from Huawei, ZTE, and others[8] by federal agency heads; as

[8] The total list of companies listed in the NDAA were Huawei Technologies Company, ZTE Corporation, Hytera Communications Corp., Hangzhou Hikvision Digital Technology Company, Dahua Technology Company.

of August 13, 2020, it will also prohibit agency heads from contracting with entities that "use" such equipment or services.[9] OMB and GSA are working together to implement these government-wide bans, and those efforts will remain pertinent to Commerce's own activities. Commerce likewise must remain attuned to any changes to that implementation process prompted by a court ruling in the pending challenge to the constitutionality of Section 889.[10]

- *FASC Exclusion Orders.* Related to the NDAA, the Federal Acquisition Security Council ("FASC") is authorized to issue "exclusion orders" prohibiting or removing certain contractors. The FASC is expected to issue interim guidance on these matters as early as January 2020.

- *Implementation of DoD Cybersecurity Maturity Model Certification.* The Department of Defense ("DoD") is currently reviewing and combining industry cybersecurity standards and best practices into one unified framework, called the "Cybersecurity Maturity Model Certification" ("CMMC") initiative.[11] Following a comment period on draft iterations of the model that spanned September through November of 2019, DoD is expected to release a final version of the CMMC (CMMC Rev. 1.0) this month, and future requests for information and for proposals at DoD will include requirements to be CMMC-certified in June and the Fall of 2020, respectively.

- *DHS Supply Chain Risk Management Task Force.* DHS's ICT Supply Chain Risk Management ("ICT SCRM") Task Force is a formally chartered partnership between industry and government that recently entered its second year of existence. Among its expected workstreams this year are a legal analysis and ensuring recommendations concerning the sharing of derogatory information on specific suppliers. These consensus recommendations will have obvious relevance to the final rules adopted in this proceeding, particularly if Commerce retains its proposed option of allowing private parties to request the initiation of an investigation under the rules.[12]

- *NTIA and NIST Initiatives on Supply Chain Security.* Both the National Telecommunications and Information Administration ("NTIA") and the National Institute of Standards & Technology ("NIST") are overseeing different processes to promote policies governing supply chain security and risk management – for instance,

[9] John S. McCain National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong., Pub. Law 115-232, 132 Stat. 1636, § 889 (2018) ("NDAA").

[10] *Huawei Technologies USA, Inc. et al. v. United States et al.*, Civil Action No. 19-159 (E.D. Tex. filed Mar. 6, 2019).

[11] Office of the Under Secretary of Defense for Acquisition & Sustainment, Cybersecurity Maturity Model Certification, https://www.acq.osd.mil/cmmc/index.html (last visited Jan. 3, 2020).

[12] *See* Information and Communications Technology Supply Chain Risk Management Task Force, *Interim Report: Status Update on Activities and Objectives of the Task Force* (Sept. 2019).

NTIA is coordinating a multistakeholder process focusing on software transparency, toward the development of a "software bill of materials."

- *Foreign Investment Risk Review Modernization Act and Export Control Reform Act.* The recent enactment of the Foreign Investment Risk Review Modernization Act ("FIRRMA") and Export Control Reform Act ("ECRA") – both of which were, like the proposed rules, specific responses to a changed national security landscape – have obvious implications for how Commerce implements the EO. Of particular note, FIRRMA expanded the authority of the Committee on Foreign Investment in the United States ("CFIUS") to monitor and review a broad range of transactions, even beyond the types of acquisitions and investments on which it historically had focused. FIRMMA also clarifies CFIUS's jurisdiction over transactions involving critical technology and infrastructure. The Treasury Department's regulations implementing FIRRMA are required to become effective no later than February 13, 2020 – presumably preceding Commerce's completion of its implementation efforts here.

To be sure, the ongoing nature of these activities will result in intangible synergies with Commerce's efforts given the overlap in substance and government/industry personnel working on them. But Commerce should not simply take for granted that coordination sufficient to avoid duplication of effort and conflicting outcomes will occur. Rather, TIA urges Commerce to highlight its role as a collaborator, rather than as a competitor, with these other government actors by expressly recognizing that these concurrent efforts are complementary to its own and will be taken into account as part of the implementation process. We recommend that the final rules make explicit the specific elements of other agencies' contributions to Commerce's implementation of these authorities. In addition, Commerce must ensure that any final rules promulgated in this docket promote the efficient and coherent implementation of these other agency actions and create a process for how Commerce's transaction reviews would be initiated, as well as a procedure for revision based on future agency actions that may need to be included. In particular, the processes for commencing a transaction review should derive from clear and formal Commerce and interagency processes, as discussed in Section III.B below.

III. THE FINAL RULES PROMULGATED IN THIS DOCKET SHOULD DEFINE AMBIGUOUS TERMS USED IN THE PROPPOSED RULES AND ESTABLISH CLEAR PROCESSES TO GOVERN COMMERCE'S NEW INVESTIGATORY AUTHORITY.

As discussed above, Commerce's proposed rules would result in an extremely broad and unprecedented increase in regulatory jurisdiction over private ICT transactions. The Notice thus marks a watershed regulatory moment for companies in or adjacent to the ICT market – which is to say, virtually every company in United States – given the government's newfound stance that it can determine key terms of what ICT companies can buy, sell, or use. As a result, this proceeding and the rules that result from it inescapably will impose additional costs on ICT companies, such as the increased practical need – even absent a legal requirement – to document supply chain risk management analysis in the event a transaction is investigated, along with related due diligence to consider the as-yet uncertain possibilities for government intervention. To that end, it is imperative that the final rules adopted by Commerce resolve ambiguous language used in the proposed rules and establish clear procedures for evaluating transactions that provide a governing blueprint for companies that find their transactions being evaluated under this newly established authority.

A. Commerce Must Clearly Define Both the Scope of Its Jurisdiction Under the Proposed Rules and the Threshold Required to Trigger Its Evaluation of a Transaction.

Given the potential increase in regulatory compliance costs on industry, it is of the utmost importance that Commerce makes compliance with these rules as clear, predictable, and manageable as possible. To that end, as Commerce promulgates a final rule in this proceeding, it must take additional steps to define or clarify ambiguous terms in the proposed rules. In particular, if Commerce is going to expand its jurisdiction over private transactions as

contemplated by the Notice, it must do so in a way that clearly sets Commerce's jurisdiction over such transactions and establishes defined criteria for warranting an investigation.

As written, Section 7.101 of the rules covers any ICT equipment/service that "involves any property in which any foreign country or a national thereof has an interest" is subject to Commerce's jurisdiction under these rules.[13] Given the global nature of the ICT industry, this sweeping language has the potential to cover *any* ICT procurement transaction – anywhere on the globe, and without regard to its actual impact on national security. The result would be to create a cloud of uncertainty over every ICT transaction, significantly impeding the growth of and innovation in this important sector.

In order to mitigate the risks and costs of compliance to industry, Commerce should consider ways to focus and target its jurisdiction under these rules on areas that are more likely to impact security. For example, Commerce should identify any part of a provider's or vendor's supply chain that would not give rise to "undue" or "unacceptable" risks. Similarly, Commerce should also establish instances or scenarios where a foreign interest would not rise to the level of jurisdiction needed to trigger a potential evaluation under these rules, such as the presence of a walled-off foreign national on an entity's board of directors, or a categorical exclusion of transactions between a U.S. company and one located in a country that is a designated U.S. ally. By taking steps in this proceeding to more clearly define the scope of the rules' intended coverage, Commerce would enhance the likelihood that it will capture those transactions that it presumably intends to scrutinize without diverting resources to those that pose no plausible national security threat.

[13] Notice at 65316.

The proposed rules also adopt as a threshold for a prohibited transaction any transaction that "poses 'an undue risk' of several specified adverse consequences, or 'an unacceptable risk' to national security or the safety of U.S. persons."[14] Any final rule established by Commerce should include the criteria that the government plans to use in determining an "undue risk" or "unacceptable risk" in order to aid industry's efforts in complying with these rules and conducting risk analyses of potential transactions. The final rules should also add clarity regarding how these terms will be interpreted, either by adopting definitions or including substantial discussion in an adopting order or other guidance about what constitutes an "undue" risk as compared to an "unacceptable" one. That guidance should include clarification as to the difference – in terms of burden of proof, penalties, and other relevant factors – between an "undue risk" and an "unacceptable risk." Should there be no meaningful distinction between the two terms, Commerce should consider eliminating "undue risk" as a distinct category in order to add additional clarity to the proceeding.

B. The Final Rules Must Establish Procedures Governing How Commerce Will Conduct Evaluations of ICT Transactions That Will Also Allow for Categorical Prohibitions and Exemptions.

Any final rules must lay out clear procedures that will allow industry to work with Commerce on evaluating potential threats posed by certain transactions. Commerce can increase the industry's willingness to aid in these evaluations by establishing a process by which the Secretary will evaluate transactions that offer notice and opportunities for companies to respond at the earliest practical moment. Similarly, Commerce can remove some of the uncertainty and breadth of these rules by establishing a process for determining that certain transactions are categorically excluded from the jurisdiction of these rules, or outright prohibited.

[14] *Id.* At 65317.

Section 7.100 of the proposed rules offers three potential triggers that could result in Commerce's review of a transaction: (1) the "discretion" of the Secretary; (2) a request "in writing … from the head of the requesting agency, or their designee;" and (3) "information submitted to the Secretary by private parties that the Secretary determines to be credible."[15] As written, however, the rules do little to provide a clear picture of how Commerce will evaluate the validity of these potential triggers in determining if an investigation is required.

The processes for commencing a transaction review under Section 7.100 should derive from clear and formal Commerce and interagency processes with established burdens of proof for launching an evaluation. Absent an exigent/emergency situation pursuant to Section 7.104 of the proposed rules, the Secretary should use his or her own discretion to commence transaction reviews under Section 7.100(a) only pursuant to a written finding of probable cause to believe the transaction in question may be subject to prohibition, mitigation, or unwinding per the criteria to assess the effect of a transaction in Section 7.101. In the event of a written request from a head of an agency or the FASC to commence a transaction review under Section 7.100(b), the request should only be granted if it articulates the head of agency's or FASC's finding of probable cause to believe the transaction in question may be subject to prohibition, mitigation, or unwinding per the criteria to assess the effect of a transaction in Section 7.101.

Most importantly, although TIA is skeptical about the utility and unintended consequences of having private parties trigger an evaluation, particularly when the Secretary already has the discretion to initiate one and can presumably take into account a private party's views in doing go in offering this route, Commerce must establish set procedures for determining whether information from private parties is "credible" under Section 7.100(c). Specifically, it

[15] *See generally* § 7.100 Commencement of an evaluation of a transaction.

should accept and act on such information only when it is provided to Commerce through legally sound processes that are currently under development in the ICT Supply Chain Risk Management Task Force. Commerce must set a high evidentiary standard for these private-party sources, in order to limit abuse by competitors or others with an incentive to use this procedure to increase an organization's costs or scuttle its commercial dealings.

Once an investigation has commenced, Section 7.101 lays out the criteria Commerce will utilize to investigate a transaction, and Section 7.102 attempts to establish a process for how an evaluation will be conducted. However, the Notice does not provide many specifics on how an investigation would proceed under Section 7.102 once commenced under Section 7.101. As currently laid out, the proposed rules introduce great uncertainty for the ICT industry, by exposing all ICT procurements dating back to May 15 of this year to the potential of being prohibited or unwound by Commerce under this new authority. At a minimum, Commerce should create a clearly articulated process, to include timelines and procedures for industry and interagency input, for reviewing potential transactions under Section 7.102.

Any procedure adopted in the final rules must afford industry (and particularly the parties to the specific transaction at issue) adequate opportunity to provide input prior to any initial determination. For example, Commerce should include a mechanism in the final rules for notifying targeted companies that a transaction is under investigation and offer an opportunity for the affected companies to submit information prior to any regulatory action. Further, any confidential or proprietary information submitted as part of an evaluation contemplated under Section 7.102 of the rules must include assurances that it will remain confidential, in order to encourage industry participation. Among other potential protections, any final rules adopted by Commerce should explicitly state that confidential and proprietary information submitted to

Commerce pursuant to these rules is presumed to qualify for protection from disclosure under the Freedom of Information Act.

In addition to establishing processes and thresholds for commencing and conducting evaluations, Commerce must also establish procedures through which various transactions could be prohibited, mitigated, or unwound under these new rules. As written, the Executive Order left open the possibility for the Secretary to determine that certain types of transactions are categorically prohibited or excluded from these rules.[16] The proposed rules, however, explicitly state that the Secretary will review transactions "on a case-by-case basis" and that the Secretary "has declined to identify classes of transactions that are subject to prohibition or are excluded from prohibition."[17] The Notice indicates that Commerce may revisit the issue, but notes only that if/when it does, "further guidance" will be issued – leaving unclear what sort of process is envisioned.[18]

TIA believes that the final rules should establish a clear and predictable mechanism by which the Secretary can identify particular classes of transactions that will be excluded from this process form the outset or that will be prohibited outright at a later date. As discussed above, this proceeding represents a profound assertion of the government's authority to review purely private commercial transactions. Even though the Secretary may decline to adopt any categorical exemptions or prohibitions at this current time, the final rules should still provide a clear mechanism for making such a determination at a later date, as well as an official avenue for stakeholders to petition Commerce to make such a determination. Any determinations for

[16] Executive Order on Securing the Information and Communications Technology and Services Supply Chain, Section 2(b) (May 15, 2019).

[17] § 7.3 Purpose.

[18] § 7.8 No categorical inclusions or exclusions.

categorical exemptions or prohibitions should also be open to industry comment, as the ICT industry would be in the best position to offer advice and information concerning these transactions. As such, the proposed rules should be revised as follows: "[s]hould the Secretary determine based on a particular case that a class of transactions should be prohibited or excluded, the Secretary *will publish such initial determination and further guidance along with a request for comment* in the Federal Register."

As a part of this mechanism, Commerce should rescind the proposed rules' prohibition on advisory opinions so that parties may have the option of socializing a potentially problematic transaction, addressing any concerns that may be presented and substantiated, and preempting any need for an investigation. Given the breadth of the proposed rules and the significant uncertainty for companies seeking to comply, it is foreseeable that companies will have a strong interest in seeking and obtaining anticipatory guidance on certain transactions in a timely manner that does not unduly interfere with their pursuit of those transactions.

That said, the mechanism for providing any such guidance should be designed in a way that alleviates the strain on Commerce's resources. With the large potential costs associated with unwinding a transaction after-the-fact, it is foreseeable that many companies will seek guidance that, in the aggregate, could inundate Commerce's existing staff. Therefore, Commerce should take steps to ensure that any guidance on transactions is limited to transactions that meet a certain threshold to be deemed substantial, such as a total value amount, and would only be subject to a brief but fixed review period – for instance, a period of no more than thirty days – after which, barring any objection by the Secretary, the transaction would be presumed not to present any undue or unacceptable risk. Finally, Commerce can further reduce the strain of

multiple requests for guidance by utilizing its discretion to create categorically prohibited and exempt classes of transactions, as discussed above.

CONCLUSION

Through this proceeding, the Department of Commerce is embarking upon an unprecedented expansion of the government's jurisdiction over private transactions between telecommunications equipment and service providers. As emphasized above, it is imperative for Commerce to continue to solicit industry feedback and work with the ICT community to ensure that these rules are properly implemented in a way that mitigates national security concerns without creating an undue burden on U.S. and U.S.-friendly business interests. To that end, TIA will continue to participate actively in all government conversations focusing on securing the ICT supply chain, including by fostering discussions with and among our member companies: the manufacturers and suppliers of the global ICT marketplace. Our member companies strive every day to ensure that ICT products are both secure and reliable, so it goes without saying that TIA has a vital stake in these efforts. We look forward to continuing our work with Commerce and the numerous other agencies involved in this broad initiative.

By: */s/ Colin Andrews*

Colin Black Andrews
Director, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Road
Suite 200
Arlington, VA 22201
(703) 907-7700

Filed: January 10, 2020