Before the
Department of Commerce
Office of the Secretary
Washington, DC 20230

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

COMMENTS OF USTELECOM—THE BROADBAND ASSOCIATION

USTelecom[1] commends the Commerce Department (Department) for engaging with industry and the interagency process to secure the Information and Communications Technology and Services (ICTS) supply chain. This opportunity for industry to provide public comment on the notice of proposed rulemaking is crucial to the Department's efforts to implement this profoundly important new authority with precision and positive effect to meet the goals of Executive Order (EO) 13873.[2]

Introduction

For years, USTelecom has played a prominent leadership role in developing and advancing U.S. cybersecurity policy in general and in the communications sector in particular. We helped the National Institute of Standards and Technology (NIST) develop the Cybersecurity Framework, and we led the Federal Communications Commission's (FCC) Communications Security, Reliability, and Interoperability Council's (CSRIC) landmark effort to implement the Framework in the communications sector. USTelecom also founded, and presently co-leads with

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives—all providing advanced communications services to both urban and rural markets.

[2] *Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed. Reg. 65316 (Nov. 27, 2019) (ICTS NPRM).

the Consumer Technology Association, the Council to Secure the Digital Economy (CSDE), a group of over a dozen large international information and communications technology (ICT) companies dedicated to preserving the security of our communications infrastructure and connected digital ecosystem. CSDE is recognized by this Administration as a leading industry partnership in coordinating efforts to combat botnets,[3] respond to cyber crises,[4] and promote IoT security.[5] Finally, USTelecom chairs the Communications Sector Coordinating Council (CSCC) and co-chairs the ICT Supply Chain Risk Management Task Force (SCRM Task Force), the two principal organizations that serve as the government's industry partners for developing cybersecurity and supply chain security policies.

USTelecom agrees with the Administration regarding the challenges we face in cybersecurity and in the global supply chain, and we recognize the security interests that are at stake in the Administration's implementation of EO 13873. With this common perspective in mind, we wish to underscore that these new authorities to intervene in private commercial transactions are truly extraordinary and unprecedented, and each action taken under this authority will have far-reaching effects in the global market for ICTS. We all have an interest in

[3] CSDE, *International Botnet and IoT Security Guide 2020*, https://securingdigitaleconomy.org/wp-content/uploads/2019/11/CSDE_Botnet-Report_2020_FINAL.pdf; *see also* U.S. Department of Homeland Security & U.S. Department of Commerce, *A Road Map Toward Resilience Against Botnets* (Nov. 29, 2018), https://www.commerce.gov/sites/default/files/2018-11/Botnet%20Road%20Map%20112918%20for%20posting_0.pdf (listing CSDE as a contributor for a variety of tasks in 2019-2020, including "Defining a Core Security Capability Baseline").

[4] CSDE, *Cyber Crisis: Foundations of Multi-Stakeholder Coordination* (Sept. 2019), https://www.ustelecom.org/wp-content/uploads/2019/09/CSDE-Report-Cyber-Crisis-Foundations-of-Multi-Stakeholder-Coordination.pdf.

[5] CSDE, *The C2 Consensus on IoT Device Security Baseline Capabilities* (Sept. 2019), https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf. The Administration has recognized these efforts. For example, Christopher Krebs, Director of DHS's Cybersecurity and Infrastructure Security Agency (CISA), has praised the CSDE and its accomplishments in his keynote speeches at the DHS CISA 2nd Annual National Cybersecurity Summit, September 26, 2019; Mobile World Congress Los Angeles 2019, October 22, 2019; and in his testimony at the U.S. Senate Committee on Homeland Security and Government Reform hearing on "Supply Chain Security, Global Competitiveness, and 5G," October 31, 2019.

getting this right, and we believe effective implementation requires ongoing and meaningful engagement between the public and private sectors to meet the Department's goals to "calibrate properly the application of this new authority" in order "to target and prohibit" only those transactions that meet the criteria of EO 13873 and "ensure that the Department does not inadvertently preclude innovation or access to technology in the United States."[6]

USTelecom is well-placed to provide constructive suggestions that will enhance the effectiveness of the proposed rules and enable the Department to take targeted action under this powerful new authority. We submit these comments in the spirit of partnership with the Department and the Administration more broadly, and with our eyes wide open about the sophisticated supply chain threats that we face together. Our recommendations derive from our belief that this foundational supply chain security regime must be built with solid cornerstones:

- Industry partnership;
- Rigorous, discerning risk analysis;
- Clear definitions of terms; and
- Interagency coordination pursuant to a sound, fair, and predictable process.

These principles imbue the observations and recommendations set forth below. Specifically, USTelecom recommends that the Department revise its proposed rules in order to achieve the following:

- Continue partnering with industry leaders and other agencies in order to promote supply chain security and leverage the expertise and institutional contributions of these public-private partnerships, by taking the steps recommended in pages 5-7 below.

[6] ICTS NPRM, 84 Fed. Reg. at 65317.

- Establish a bright-line approach similar to the Export Administration Regulations' "Entity List" by publishing a list (or alternatively, policy guidance with unmistakably clear criteria) of persons or governments that are "foreign adversaries" that provide ICTS, in order to draw clearer lines between prohibited and permitted transactions and better focus the scope of transaction evaluations, as specified in the recommendations listed in pages 10-12 below.
- Coordinate the Department's transaction evaluations formally with other agencies at every step and enhance the level and quality of such interagency coordination, by adopting the recommendations listed in pages 13-14 below.

Discussion

I. USTelecom Urges the Commerce Department to Continue Partnering with Industry Leaders and Other Agencies to Promote Supply Chain Security

As we have stated publicly and demonstrated through our own work, we believe deeply in formal collaborative efforts between industry and the various agencies of our federal government. These partnership efforts should feed into the Department's implementation of the final rules; indeed, this is the only approach that will be effective in securing the ICTS supply chain.

In particular, the rules should recognize the roles of the Sector Coordinating Councils and the SCRM Task Force and their substantial work on supply chain security, including work required by EO 13873 itself. In particular, the CSCC engaged meaningfully with DHS in contributing to the security assessment required under Section 5(b) of EO 13873, and going forward, industry—through the CSCC, IT-SCC, and other Sector Coordinating Councils—should have clear and significant responsibilities and expectations under the rules to continue to contribute to future updates of this annual assessment, as well as future additional assessment

that address other sectors. The SCRM Task Force, the only formal industry-government collaboration on supply chain security, is presently beginning to develop formal recommendations for legal and procedural mechanisms to govern industry's sharing with government of information regarding specific suppliers and transactions.[7] These recommendations, in the form of specific regulatory or legislative proposals intended to address existing information-sharing barriers, could address existing legal and procedural gaps that may handicap the Department's effective implementation of its new authorities under EO 13873.

Generally, USTelecom urges the Department to leverage the expertise and institutional contributions of these public/private partnerships in every aspect of its implementation of these authorities. To that end, we provide the following specific recommendations.[8]

- The final rules should articulate specifically how these existing processes feed into Commerce's commencement of, criteria for, and conduct of evaluations of transactions under §§ 7.100-7.102. For instance, we recommend that the CSCC, the IT-SCC, other pertinent SCCs (*e.g.*, in an evaluation that involves the energy or financial sectors), and the SCRM Task Force should be formally notified of any preliminary determinations under proposed rule § 7.103 and should have the opportunity to provide input to the Department prior to a final determination. Such input should include analysis of the transaction's pertinence to the risks identified in the DHS criticality assessment, without compromising confidentiality.
    - The opportunity to provide this input is essential to the extent that a particular determination may become "precedent" for subsequent transactions (at least those presenting similar circumstances). Despite the "case-by-case" approach contemplated by the Department, we expect that over time the issuance of determinations will lead to the development of a sort of "common law" that the Department and industry may wish or feel compelled to cite in support of or against certain outcomes.
    - Given the likelihood that a determination on a specific transaction may have impact beyond that transaction and thereby more generally affect future industry supply-chain decisions, the Department will be best served by affording industry

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

[8] Section III below, regarding the need for greater procedural clarity, contains additional recommendations that are pertinent to industry-government engagement.

an opportunity to participate in the development of each such precedent from the outset so that the Department can be informed of any broader considerations (*e.g.*, impact on consumers or U.S. technological leadership) and the potential repercussions of its decisions for the industry at large. Such input could help the Department avoid unnecessary industry or consumer impact by adopting mitigation requirements and/or transition timeframes in lieu of outright and immediate bans on particular transactions. We expect industry stakeholders will be able to provide that insight without compromising the confidentiality of the transaction in question.

- The final rules should also revise § 7.7 to allow for engagement between industry and Commerce about suspect transactions, under the legal processes presently being developed by the SCRM Task Force, to lead to broad advisory opinions that provide clarity to companies wishing to abide by these rules. Such opinions will provide industry constructive notice of the government's security concerns, thereby allowing us to make supply-chain decisions with knowledge of those concerns, as opposed to finding them out after we have closed a transaction. Possible models for individual companies include notice filings with the Committee on Foreign Investment in the United States (CFIUS) regarding planned acquisitions or voluntary disclosures to the Bureau of Industry and Security (BIS) regarding export irregularities. However, we recommend against creating new regimes for licensing or transaction "pre-approval" due to the burden such a regime would place on Department staff and on industry.

- We recognize that the Department may need to initially (and privately) investigate the credibility of a complaint before alerting the affected parties that a transaction is under investigation. However, as a matter of fairness, the Department should not come to any "preliminary decision" before giving the parties to the transaction an opportunity to respond. Any "preliminary" finding should be limited to a finding that there is legitimate reason to move forward with an investigation, not a preliminary decision on the merits. The Department should be careful not to prejudge a transaction before parties have notice and an opportunity to respond.

- While industry input is critical to the effectiveness of the Department's regime, the Department should not allow its process to be abused. Thus, as discussed below in Section III, if the Department is inclined to retain § 7.100(c) (regarding private party information prompting a transaction evaluation), it should place restrictions on the availability of this mechanism to ensure that it is reserved for truly credible threats and cannot be misused for retaliatory or other purposes that are independent of any national security risk. For example, the rule could require that a private party must provide notice of any complaint filed with the Department to affected parties.

- More broadly, Commerce could work collaboratively with industry toward a competitive and secure supply chain, for example, through periodic government-and-industry briefings or workshops to share concerns and receive industry input, similar to the Annual Conference on Export Controls and periodic seminars that the Bureau of Industry and Security hosts. This would avoid surprises, allow industry input, and put the industry

on notice if the Department has concerns about particular companies or types of transactions.

II. USTelecom Urges the Commerce Department to Establish a Bright-Line Approach Similar to the Export Administration Regulations' "Entity List," Relying on the DHS Risk Assessment and Related Tools to Draw Lines Between Prohibited and Permitted Transactions

The present scope of the proposed rules covers virtually every conceivable ICTS transaction. Absent changes that provide for clarity regarding possible actions under this authority, these rules would create significant new business unpredictability and risk that would impair decision-making and deal-making by U.S. companies on investments, sourcing, and collaborations on research and product development with law-abiding foreign entities that are the norm in the ICT industry.

Without clear guidance on which industry can rely, the rules would create unmanageable uncertainty for industry and our economy generally, as well as potentially devastating consequences for individual parties that make discerning but unlucky choices about ICTS procurements. Such apparent arbitrariness is not conducive to prosperous commerce or to supply chain security, especially where long-established practices concerning vetting and risk management might be drawn into question for the first time, both prospectively and retroactively. This uncertainty would severely disadvantage U.S. companies vis-à-vis foreign competitors and could disrupt business relationships throughout the complex global ICTS market that presently benefit companies in every sector of the U.S. economy. The final rules should therefore focus the scope of these new authorities on specific ICTS that could present specific significant risks to critical functions performed in various sectors.

Moreover, creating an entirely new regime of tremendous breadth and scope resting exclusively on a "case-by-case" approach to evaluating transactions would not contribute to

clarity on these important issues. Without conceptual guidance and clear definitions and criteria describing issues such as what entities are "foreign adversaries" and what types of transactions create national security risks, the need for advisory guidance (discussed below) will be even more urgent, and the burdens on the Department all the greater. The private sector would likely bring a massive number of transactions to the Department for evaluation, many of which will likely be deemed permissible. The Department, in turn, would risk being overwhelmed by evaluating and providing guidance on benign transactions, which would pull resources and attention away from the smaller number of closer calls that require complex legal and factual analysis.

Therefore, USTelecom recommends revising the rules in ways that promote regulatory certainty and establish a workable process both for the Department to administer and for industry to follow by publishing a list—or, alternatively, policy guidance with unmistakably clear criteria—of persons or governments that are "foreign adversaries" that provide ICTS. This would give industry "bright line" awareness regarding prohibited transactions that would create much-needed predictability; simply avoiding transactions with such entities would ensure compliance with the rules.

For the next step, the Department, in coordination with other agencies, the CSCC, the IT-SCC, and the SCRM Task Force, should leverage existing tools such as DHS's criticality assessment to clarify the types of transactions that:

- Meet the criteria in 7.101(a)(5), whether appropriately addressed through prohibitions or mitigation;
- May be permissible with persons on the foreign adversary list if appropriately mitigated; or
- Are generally unlikely to implicate the "undue" or "unacceptable" risks contemplated in the rules and are presumed permissible.

This approach is consistent with existing, workable approaches for administering technology transfer regimes, including the EAR and the customs rules. For example, the EAR's Entity List in Supplement 4 to Part 744 contains a list of entities and specific licensing requirements for each entity, along with licensing review policies. At this stage of the development of this nascent regulatory regime, the processes need not—and should not—be as rigid as the EAR's licensing regime. However, establishing clear guidance through formal iterative processes with relevant interagency and industry stakeholders would provide significant advances in the Department's and industry's mutual approaches to addressing these risks.

To that end, regardless of the mechanics of the Department's review of transactions, the Department should issue general guidance regarding transactions with a person on the foreign adversaries list that involves ICTS that does not put national security or any critical infrastructure at risk. The starting point for such a list should be those products and services that DHS has deemed "non-critical" in its criticality assessment, and the Department should initiate an ongoing process to flesh our additional permissible transactions guidance that may be appropriate.[9] The Department could also eliminate uncertainty by designating a small set of countries that are not foreign adversaries, such as those with joint defense agreements with the U.S.

The Department should also, again with Sector Coordinating Council input and in coordination with other agencies, create a process whereby a transaction involving a potentially critical input into the ICTS supply chain may nevertheless be permissible if the risks to national security are appropriately managed. This is consistent with, and can be informed by, DHS's

[9] DHS contemplates an additional work stream that would involve performing a similar criticality assessment for ICTS used by critical infrastructure sectors other the communications sector. The Department could work with DHS to develop, in conjunction with private sector input, additional guidance for transactions involving products sold into other critical infrastructure sectors.

criticality assessment, which breaks down inputs into the communications sector into "non-critical," "manageably critical," and "critical." For transactions that involve products or services that are "manageably critical," the Department should permit parties looking to purchase such products or services to submit their transactions to the Department and obtain "advice letters" or other guidance about whether they likely comply with the rules.[10]

Shifting the proposed regime to this approach would substantially increase regulatory certainty, reduce the risk of unintended consequences, and help focus the Department's resources on those transactions that require significant attention and analysis. To advance this general approach and to help reach the Department's stated goals to "calibrate" and "target" particular transactions of concern as reiterated above, we provide the following specific recommendations to focus the scope of transaction evaluations.

- In accordance with NDAA Section 889, revise § 7.8 to categorically exclude from the scope of transaction evaluations: (1) a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements, or (2) telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

- In accordance with longstanding statutory processes, revise § 7.8 to categorically exclude from the scope of transaction evaluations of any transactions that have previously undergone (or are undergoing) a national security review by CFIUS, by Team Telecom, or pursuant to the EAR.

- Eliminate the possibility of unwinding transactions retroactively; instead, create a collaborative process by which a company can work with Commerce and other agencies to mitigate the risks of any transactions that in the future may call for evaluation or remediation.

- Specify the depth of the rules' reach into ICTS hardware and software subcomponents. In the first instance, we strongly recommend that transaction evaluations begin with transactions regarding end items only. In the future, the Department could leverage the

[10] This process will mean relaxing the Department's proposed policy against issuing advisory opinions or declaratory rulings. Relaxing that proposal is necessary in order to effectively create a body of guidance that provides private sector entities with sufficient regulatory certainty.

ongoing work being done in DHS, the SCRM Task Force, and other arenas to develop a framework for addressing subcomponents.

- In § 7.1(a)(1), "subject to the jurisdiction" should be defined to limit the extraterritorial effects of the rule on international transactions. It is USTelecom's understanding—and recommendation—that the purpose of these rules is to secure the U.S. ICTS supply chain and U.S. networks, rather than to create a regime with extraterritorial effects.

    - The preamble of EO 13873 itself states that the EO's goal is "to protect the security, integrity, and reliability of information and communications technology and services provided and used in the United States."[11] That goal is consistent with the statutory authority underlying the EO, the International Emergency Economic Powers Act (IEEPA), which permits a president to "deal with any unusual and extraordinary threat … to the national security, foreign policy, or economy of the United States" and limits its scope to persons or property "subject to the jurisdiction of the United States."[12]

    - In addition, the dominant telecommunications equipment vendors differ significantly inside and outside the U.S. As a result, there are differing policy considerations at play when considering the impact, both to the industry and consumers, of banning particular transactions outside versus inside the U.S.

    - This domestically oriented purpose should be made explicit in the final rules to guard against any questions of extraterritorial impact of Department determinations. To the extent the Administration seeks to protect the global supply chain, it can (and should) continue to utilize other mechanisms, including existing trade laws and ongoing Administration efforts to convince U.S. allies to emulate security measures taken by the U.S.

- In § 7.1(a)(2), "interest" should be defined to limit the scope of evaluations to transactions where a foreign entity has a controlling interest in the underlying property, and should exclude de minimis interests, such as a bank financing an entity through a letter of credit or minority or non-controlling interests.

- In § 7.2, "foreign adversary" should be defined to exclude companies legally chartered and governed by the laws of a government with whom the United States has a defense alliance based on a treaty or other formal agreement. The definition should further describe the distinctions between foreign adversaries that are governments and those that are non-government entities.

- In § 7.2, the definition of "transaction" should delete "dealing in," as this term is either unclear or redundant, and should define "use of" in accordance with that term's meaning in Section 889 of the National Defense Authorization Act of 2019.

[11] EO 13873.

[12] 50 U.S.C. § 1701(a).

- In § 7.101(a)(5), "undue risk" and "unacceptable risk" should be defined terms. Moreover, the Department should consider using only one of those two terms.

III. USTelecom Urges the Commerce Department to Coordinate Its Transaction Evaluations Formally with Other Agencies at Every Step

The U.S. government is presently engaged in multiple other significant efforts of various scope and maturity to promote the security of the ICTS supply chain, particularly in the communications sector. A number of these policy activities are directly pertinent to the Department's implementation of the authorities in EO 13873 and to the SCRM Task Force's ongoing work. These include a several initiatives focused on procurement, such as the implementation of prohibitions on procurement from specific suppliers in Section 889 of the National Defense Authorization Act of 2019 by the General Services Administration and the Department of Defense (DoD); DoD's concurrent development and implementation of a Cybersecurity Maturity Model Certification (CMMC) program for defense contractors; and rules from the Federal Acquisition Security Council regarding "exclusion orders" for federal procurement. Meanwhile, other agencies are pursuing initiatives that will also impact industry and influence the Department's efforts—most notably, the FCC's implementation of prohibitions on the use of federal money to purchase certain suspect equipment and services and exploration of additional restrictions. And NTIA is overseeing a multistakeholder process to enhance software supply chain security through the development of a "software bill of materials" or "SBoM."

To promote the coherence of the "whole of government" approach to ICTS supply chain security and to maximize the impact of industry's real-world implementation of ICTS supply chain risk management measures, the Department should implement its new transaction evaluation authority in coordination with these related supply chain security activities. The

Department's actions regarding specific transactions will affect these other processes—and vice versa.

The initial proposal's interagency consultation requirement in § 7.101 evidences the Department's recognition of the important perspectives that these coterminous proceedings and initiatives, but we think the Department can go further by spelling out this consultation process in greater detail—for instance, by requiring that it include written input from other agencies regarding their analyses and assessments regarding undue/unacceptable risk.

Additionally, we recommend the following revisions to the proposed rules to enhance the level and quality of interagency coordination that the Department will need to implement its new authority more effectively:

- When using his "discretion" to commence a transaction evaluation under § 7.100(a), the Secretary should provide the other heads of agency identified for consultation in § 7.101 formal written notice of the transaction evaluation. This notice should include an explicit tie to the DHS criticality assessment (which DHS is annually updating and improving with CSCC input), the factual and analytical basis of the need for an evaluation, and a proposed schedule of interagency consultation.

- To commence a transaction evaluation pursuant to a "written request" under § 7.100(b), the Secretary should grant requests for a transaction evaluation from other heads of agency or the Federal Acquisition Security Council only in response to a request similar in form and substance to the formal written notice described above through which the Secretary would exercise his own discretion to commence a transaction. The Secretary should then provide notice to the other heads of agency of his decision to grant the request.

- As noted above, the SCRM Task Force is presently developing recommendations for legal mechanisms and processes to protect against potential abuses of opportunities to share information with the government. Such recommendations will not be complete until mid-2020 at the earliest, and they likely will include legislative or regulatory policy proposals that would need to be implemented subsequently. Encouraging private parties to provide information about certain suppliers or transactions under these rules prior to consideration of these currently developing proposals would be premature and could lead to abuse by competing suppliers. Therefore, USTelecom recommends that either:

- The final rules should altogether delete § 7.100(c) regarding the commencement of an evaluation based on "information submitted to the Secretary by private parties that the Secretary determines to be credible;" or

- As an alternative that could promote industry-government collaboration of the type described above in Section I, the Department could retain the general option contemplated by § 7.100(c) but revise it to (i) require that parties seeking to utilize this mechanism satisfy a higher evidentiary standard, (ii) limit eligibility to use this mechanism to a particular category (*e.g.*, U.S. or allied persons proposing to purchase ICTS, but not third parties), and/or (iii) provide for greater transparency in order to reduce incentives to initiate a request for an evaluation for malicious or anti-competitive reasons, such as requiring that private parties providing information to the Department also provide notice to affected parties. The bottom line is that the Department should guard against creating a process that supplies competitors or disgruntled suppliers with a weapon to disrupt the ICTS market in pursuit of their own commercial interests.

- As noted above, the Secretary should provide parties to a transaction notice and an opportunity to provide comment upon the commencement of an evaluation under § 7.100—that is, prior to any decision, preliminary or final.

- The Department should clarify the specific procedural steps through which it will receive input from parties to the transaction, other private experts or sources of information or analysis, and its interagency partners in the conduct of an evaluation under § 7.102.

- As recommended above, the CSCC, the IT-SCC, and other pertinent SCCs (for instance, in an evaluation that involves the energy or financial sectors), along with the SCRM Task Force, should be formally notified of any evaluations or determinations under § 7.103 and should have the opportunity to provide input to the Department prior to a final determination. Additionally, this notice and comment opportunity should also include the Department's interagency partners. Among other benefits, such a process would give other stakeholders an opportunity to shape precedent in this area as it evolves and begins unavoidably to influence future transactions.

- The proposed rules do not include any deadline for the Department to issue a final determination when conducting an evaluation. This creates additional uncertainty for the private sector that could cause harm by substantially chilling private commerce. Accordingly, the Department should establish a reasonable time frame for making determinations (*e.g.*, 30 days or 60 days).

Conclusion

Again, USTelecom commends the Department for engaging with industry and the interagency to secure the ICTS supply chain. This opportunity to provide constructive

suggestions is crucial to efforts to implement this profound and extraordinary new authority with precision and positive effect to meet the goals of EO 13873. USTelecom is dedicated to the government-industry collaboration that will be necessary to secure the global ICTS ecosystem, and we submit these comments pursuant to our spirit of partnership with the U.S. and allied governments. We are fully aware of the threats that we face together. To that end, in summary, USTelecom urges the Commerce Department to:

- Continue partnering with industry leaders and other agencies to promote supply chain security;
- Establish a bright-line approach similar to the EAR's "Entity List," relying on the DHS risk assessment and related tools to draw lines between prohibited and permitted transactions; and
- Coordinate its transaction evaluations formally with other agencies at every step.

* * *

These suggestions derive from our belief that this foundational supply chain regime must be built with solid cornerstones: Industry partnership; rigorous, discerning risk analysis; clear definitions of terms; and interagency coordination pursuant to a sound, fair, and predictable process. We stand ready to work with the Department and other key stakeholders in industry and government to advance the security of the ICTS supply.

/s/ Robert Mayer

Robert Mayer
Senior Vice President, Cybersecurity
USTelecom – The Broadband Association
601 New Jersey Avenue, NW, Suite 600
Washington, DC 20001
(202) 326-7300

/s/ Michael Saperstein

Michael Saperstein
Vice President, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue, NW, Suite 600
Washington, DC 20001
(202) 326-7300

January 10, 2020