Business Roundtable

1000 Maine Avenue, SW, STE 500
Washington, DC 20024
202.872.1260
www.brt.org

March 22, 2021

BY ELECTRONIC SUBMISSION AT: *https://www.regulations.gov*

RE: DOC-2019-0005; RIN 0605-AA51; Comments to the Interim Final Rule on Securing the Information and Communications Technology and Services Supply Chain

Business Roundtable, an association of chief executive officers who collectively lead companies with more than 20 million employees and more than $9 trillion in annual revenues, welcomes the opportunity to provide comments to the "Securing the Information and Communications Technology and Services Supply Chain" Interim Final Rule ("IFR") as requested by the Department of Commerce Federal Register Notice dated January 19, 2021. Despite some improvements, significant changes are needed to improve the IFR's clarity and efficacy, and to avoid potentially significant unintended consequences to the U.S. economy. Business Roundtable respectfully requests that the Department of Commerce extend the IFR's effective date until after the new Administration has had sufficient time to engage with key stakeholders and further refine and better target its approach.

Securing the information and communications technology and services ("ICTS") supply chain is vital to the U.S. economy and U.S. national security. Business Roundtable supports the intent of the IFR to enhance ICTS supply chain security. On January 10, 2020, Business Roundtable submitted comments on the November 2019 Proposed Rule expressing concerns that the then-Proposed Rule would prove unworkable and undermine U.S. innovation leadership and economic strength without achieving its national security and ICTS security objectives (see attached). Business Roundtable appreciates the U.S. Government's efforts to address our earlier comments and the IFR improves the Proposed Rule in some areas. Business Roundtable continues, however, to have a number of fundamental concerns with the IFR. In its current form, the IFR could significantly disrupt the U.S. economy and would not best advance its intended national security objectives.

We appreciate that the IFR now identifies specific foreign adversaries, limits the retroactivity of the authority, recognizes the need for a safe harbor option, and provides greater transparency to the review process by providing affected parties notice and an opportunity to be heard. These adjustments, however, represent only incremental improvements to the Proposed Rule, and they do not sufficiently resolve the rule's fundamental lack of clarity and overly expansive scope:

- The IFR remains overly broad with respect to the scope of covered ICTS transactions. The six newly-identified categories of covered technologies remain too broad to provide adequate guidance to affected U.S. companies regarding the intended scope of the rule.

- The IFR does not identify any categorical exclusions, such as for mass market electronic devices and commercial off-the-shelf items. Such exemptions are needed to permit low risk transactions to continue to facilitate economic growth without the undue and unclear threat of regulatory intervention.

- The IFR subjects transactions to multiple, redundant, and potentially conflicting regulatory reviews and does not exempt transactions that are subject to other U.S. regulatory reviews involving an assessment of national security risks – for example, all transactions subject to the Committee on Foreign Investment in the United States, not just those that are under or have been reviewed; export controls; and Team Telecom review.

- The IFR does not define vague terms such as "interest" in property, "dealing in," or "use of."

- The IFR does not tie the rule's scope to any specific threat or vulnerability identified in a public U.S. government assessment.

- The IFR does not clearly limit the application of penalties for violations of final determinations to the specific parties to the transaction that is the subject of the Commerce action. Penalties for violations of a final determination, mitigation agreement, or other direction issued under the ICTS regulations should be assessable only against the specific parties to the subject transaction and not third parties that may be indirectly involved (e.g., through shipping, financing, insuring, etc.).

These deficiencies in the IFR present U.S. companies and their customers and suppliers with significant questions and insufficient information to comply with the rule's requirements, which could result in both under- and over-compliance with the rule. The IFR would subject U.S. companies to potentially unnecessary and costly compliance burdens that could undermine this Administration's efforts to promote U.S. jobs and economic recovery. Conversely, other transactions that do pose a legitimate national security risk could go unaddressed unless specifically identified by Commerce, thereby diminishing the rule's impact on effectively mitigating national security risks to the ICTS supply chain.

Moreover, some of the IFR's changes from the Proposed Rule have introduced new concerns and added layers of needless complexity to the rule. For example, the six-month timeline provided to reach a final determination regarding a specific business transaction is not aligned with commercial realities of a typical ICTS transaction. The Commerce Department estimates that the IFR could potentially affect millions of businesses and result in significant compliance costs estimated between $1 billion and $53 billion – and annualized costs between $235 million

and $20 billion. Business Roundtable respectfully requests that the Administration undertake a closer collaboration with U.S. industry stakeholders to better understand the full impacts of the IFR on U.S. companies and the U.S. economy before it takes effect. We recommend:

- Leaving the comment period open beyond March 22 to allow for additional feedback on recommended substantive and technical fixes to the IFR.

- Holding town halls and public meetings to hear directly from impacted U.S. companies and to provide an opportunity for Q&A with the Commerce officials who will administer the IFR.

- Extending the IFR's effective date until the new Administration has had sufficient time to engage with key stakeholders and further refine and better target its approach.

Thank you for consideration of these comments. Business Roundtable appreciates the opportunity to continue working with the Administration on its ICTS supply chain security efforts.

Attachment:

- January 10, 2020 [Docket No. 191119-0084] RIN 0605–AA51; Business Roundtable Comments to Proposed Rule on Securing the Information and Communications Technology and Services Supply Chain

Business Roundtable

1000 Maine Avenue, SW, STE 500
Washington, DC 20024
202.872.1260
brt.org

January 10, 2020

BY ELECTRONIC SUBMISSION AT: *http://www.regulations.gov*

RE: [Docket No. 191119-0084] RIN 0605–AA51; COMMENTS TO PROPOSED RULE ON SECURING THE INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES SUPPLY CHAIN

As requested by the Department of Commerce Federal Register Notice dated November 27, 2019, "Securing the Information and Communications Technology and Services Supply Chain," Business Roundtable, an association of chief executive officers who collectively lead companies with more than $7 trillion in annual revenues and nearly 15 million employees, is providing comments to the Proposed Rule. We appreciate this opportunity.

Business Roundtable shares the Administration's commitment to securing the information and communications technology and services (ICTS) supply chain. The ICTS supply chain is critical to U.S. economic growth, innovation, competitiveness and national security. As the Administration works to implement Executive Order 13873 to secure the ICTS supply chain, it should focus on clearly identified national security threats and adopt a transparent, targeted and clear regulatory regime.

The Proposed Rule, as written, could result in significant economic harm to the U.S. ICTS sector and unrelated industries without producing the intended national security benefits. Specifically, the Proposed Rule:

- Covers almost any ICTS business activity with an international nexus due to its broad scope.

- Delegates broad and ill-defined "case-by-case" authority to review and block a broad swath of transactions without a meaningful published standard of review and no notice of the types of transactions that could be subject to the new regime.

- Lacks a pre- or post-transaction clearance process and provides parties no means of determining whether a transaction could fall within the new regulatory regime and thus be subject to mitigation requirements or transaction prohibitions after the transaction has been completed.

If implemented in its current form, the Proposed Rule will create uncertainty and confusion that could undermine both U.S. competitiveness and national security objectives. Foreign partners will do less business with U.S. companies given the open-ended risk that a wide range of completed transactions could fall within the Proposed Rule regime and be disrupted without

notice. Such an approach could weaken U.S. economic leadership and competitiveness in the ICTS sector and undermine the national security benefits of this leadership.

Respectfully, the Proposed Rule is unworkable for U.S. businesses in its current form and should not be considered for final publication without significant revisions that incorporate industry engagement and comments.

At a minimum, Commerce should publish a second Proposed Rule for notice and comment that:

1. Identifies more specifically the types of transactions that would be covered and excluded by the rule;

2. Establishes a specific set of criteria to designate foreign adversaries and specifically identifies such adversaries;

3. Describes the specific equipment of concern;

4. Avoids redundancy with existing national security statutory and regulatory regimes by exempting transactions covered by those regimes;

5. Focuses on future and pending transactions if a national security risk is identified; and

6. Contains an optional safe harbor process so that parties can have confidence that covered transactions will not be unwound or altered after completion.

Given the breadth of the Executive Order and the Proposed Rule, we strongly encourage the Administration and the Department of Commerce to work closely with the U.S. business community on the design, development and implementation of a new ICTS supply chain regulatory regime through an iterative process to advance our shared objective of protecting national security, economic prosperity and innovation leadership.

###

The following sections below respond directly to the questions posed in the Federal Register Notice and provide additional comments and recommendations for revising the Proposed Rule.

I. TRANSACTIONS POTENTIALLY COVERED BY THE PROPOSED RULE

The Proposed Rule should focus on specific national security risks in the ICTS sector that are not currently subject to regulation under other national security statutory regimes. But the lack of clarity and parameters in the Proposed Rule could enable it to reach a broad range of low-risk transactions that fall well outside any gaps in existing regulatory or statutory frameworks.

Without further clarification, under the Proposed Rule any U.S. person using a cell phone either in or outside the United States could conceivably be subject to the Proposed Rule regime. Or a U.S. company importing electronics components from its wholly owned non-U.S. subsidiary

could fall within the regime. The Proposed Rule also could reach financial transactions for the importation of electronics between a non-U.S. subsidiary and its U.S. parent or even the sale abroad by a U.S. person of foreign-made electronic components.

Commerce should issue a second Proposed Rule that significantly clarifies and narrows the scope of transactions subject to these rules.

II. RESPONSES TO FEDERAL REGISTER NOTICE QUESTIONS

In the following paragraphs, we provide comments solicited in Section III of the Federal Register Notice. We hope that Commerce will address these concerns in a second Proposed Rule to create a more focused and transparent framework.

a. Are there instances where the Secretary should consider categorical exclusions? Are there classes of persons whose use of ICTS can never violate the Executive order? If so, please provide a detailed explanation of why the commenter believes a particular transaction can never meet the requirements of the Executive order.

Meaningfully identifying and suggesting categorical exclusions is difficult, if not impossible, for industry without more information about the specific threats and vulnerabilities targeted by these regulations. Bearing that in mind, we offer the following comments:

- Commerce should categorically exclude transactions that lack a nexus to a specific threat or vulnerability articulated in public U.S. government assessments that Commerce identifies as a potential basis for action under this Proposed Rule. Such an approach should begin by providing notice to parties of the specific types of transactions that may be targeted for review under the Proposed Rule and allowing them to take steps proactively to mitigate or avoid national security risks. This step would reduce the risk of unnecessary economic harm to U.S. companies and U.S. persons in the ICTS sector while also preserving the government's ability to address the legitimate national security risks articulated in the Executive Order. Categorical exclusions could include but should not be limited to mass market electronic devices and commercial off-the-shelf items.

- Commerce should exclude from the Proposed Rule any transactions that have been reviewed and approved through other U.S. government processes that involve an assessment of national security risks (e.g., Committee on Foreign Investment in the United States (CFIUS), export controls, Team Telecom and others). Existing statutory authorities that cover specific ICTS transactions should pre-empt the application of the authority outlined in the final rule pursuant to the Executive Order. Similarly, transactions that have been reviewed by Commerce under the Proposed Rule and have not been prohibited or mitigated should not be subject to further review by Commerce absent notice to the principal parties and the establishment of significant changes to facts and circumstances affecting the transaction.

- Commerce should refine the scope of transactions covered by revising 101(a)(2). The scope of this authority should be limited to transactions directly involving "foreign adversaries" and not to "any foreign country or national" with an "interest" in the transaction. Furthermore, "interest" should be defined narrowly to include only current interests that afford the foreign party actual physical control or access to ICTS.

- Commerce should clarify that no allied country will qualify as a "foreign adversary" under this rule. Commerce should exclude transactions within the jurisdiction of an allied country. For a party owned or controlled by a company headquartered in the United States or an allied country (e.g., Wassenaar, North Atlantic Treaty Organization, etc.), merely being "subject to the jurisdiction" of a "foreign adversary" alone should not subject parties to the new regulatory regime. Foreign subsidiaries of U.S. and allied companies do not pose the same risks as companies that are owned or controlled by a foreign adversary.

- Commerce should also limit the scope of persons covered by limiting the transactions "conducted by any person subject to the jurisdiction of the United States" in Proposed Rule § 7.1(a)(1). Mere involvement of a U.S. person, such as an employee or third party, in supporting an international transaction should not subject that person to review of his or her involvement by Commerce. The U.S. jurisdictional nexus should be limited to the principal parties of the transaction to avoid inappropriate extraterritorial reach. The definition of "transaction" should not include mere use by a person subject to U.S. jurisdiction.

- Commerce should limit the scope to principal parties in a covered transaction. Commerce should clarify that entities that are not parties to the transaction under review, such as a common carrier or other intermediary, will not fall within the scope of the new regulatory regime or be held liable for providing transportation, delivery or other incidental services related to a transaction that may be subject to this framework as they are not a party to the covered transaction.

b. Are there transactions involving types or classes of ICTS where the acquisition or use in the United States or by U.S. parties would fall within the terms of the Executive order's prohibited transactions because the transaction could present an undue or unacceptable risk, but that risk could be reliably and adequately mitigated to prevent the undue or unacceptable risk? If the commenter believes the risks of a prohibited transaction can be mitigated, what form could such mitigation measures take?

This question cannot be fully answered unless Commerce identifies with much greater specificity the threats and vulnerabilities the Proposed Rule aims to address; however, mitigation should always be the first option for parties whose transactions are covered in the final regulatory regime. To that end, we offer the following comments:

- Commerce should establish mitigation procedures and take into account steps U.S. companies take to mitigate risk in other existing statutory national security regimes. Moreover, mitigation efforts taken to comply with other statutory and regulatory regimes, such as CFIUS, should pre-empt and satisfy mitigation requirements for a new regulatory regime. Existing statutory authorities that cover specific ICTS transactions should pre-empt the application of the authority outlined in the final rule pursuant to the Executive Order.

- Commerce should account for and provide benefits and exclusions for parties that meet approved supply chain risk management standards and participate in U.S. supply chain programs (e.g., Department of Homeland Security ICT Supply Chain Risk Management Task Force).

- Commerce should adopt the least intrusive measures necessary to mitigate the risks involved in a particular covered transaction. Commerce always should consider and give strong preference to allowing mitigation measures over blocking a covered transaction. Only in exceptional circumstances, where no mitigation measures are reasonably available, should Commerce consider blocking a transaction. Blocking and mitigation should be limited strictly to addressing specific national security threats and not apply to other broader foreign policy or economic policy objectives.

    c. ***If mitigation measures are adopted for a transaction otherwise prohibited by the Executive order, how should the Secretary ensure that parties to such transaction consistently execute and comply with the agreed-upon mitigation measures that make an otherwise prohibited transaction permissible? How best could the Secretary be made aware of changes in factual circumstances, including technology developments, that could render mitigation measures obsolete, no longer effective, or newly applicable****?***

Commerce should look to other existing regimes (e.g., CFIUS, export controls, Team Telecom, and others [) for examples of mitigation enforcement and monitoring procedures (e.g., reliance on the use of internal security officers, third-party monitors, auditors, and other industry best practices). Importantly, Commerce should also be required to adopt the least burdensome steps necessary to mitigate the designated national security risk for a covered transaction.

    d. ***Section 1(a) of the Executive Order and the definition of ''transaction'' that the proposed rule would implement refer to ''acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service.'' How are these terms, in particular ''dealing in'' and ''use of,'' best interpreted?***

In general, Commerce should define terms in the rule (e.g., "acquisition," "importation," "installation") according to industry-accepted or dictionary definitions to ensure consistent application to all parties.

Commerce should also exclude the terms "dealing in" and "use of" from the definition of "transaction" as these terms capture activities that go far beyond what would be considered a transaction in common usage. Alternatively, at the very least, "dealing in" and "use of" should be linked narrowly to specific threats and vulnerabilities and not capture general use or dealing in ICTS items.

e. As discussed above, the Secretary expects persons engaged in transactions will maintain records of those transactions in the ordinary course of business. Should the Department require additional recordkeeping requirements for information related to transactions?

Commerce should not impose any additional recordkeeping requirements for information related to ICTS "transactions" as defined in the draft regulations. Commerce should follow the model of numerous other regulatory regimes — including its own in the Export Administration Regulations — by requiring the retention only of records created or maintained in the ordinary course of business.

III. ADDITIONAL COMMENTS

a. Do not apply retroactively between May and the effective date.

Consistent with other Proposed Rules issued under similar authorities and for similar national security purposes, Commerce should not extend the scope of the new regulatory regime to transactions undertaken since the May 15, 2019, effective date of the Executive Order. The application of retroactive authority over transactions completed since May could result in takings without prior notice, particularly given the continued lack of clarity as to what transactions are subject to the Executive Order.

b. Establish an optional process for pre- and post-transaction clearance and review.

Consistent with other related regimes, Commerce should establish an optional mechanism for obtaining pre-clearance for potentially covered transactions through a voluntary notification process. If Commerce does not respond to the notification within a reasonable time, the transaction should be given a safe harbor. Along the same lines, Commerce should provide for advisory opinions to give industry guidance to anticipate potential risks to its supply chain and improve compliance and risk mitigation.

c. Establish regular congressional consultations to implement the new regime and clear requirements and guidance to limit withholding of notice to affected parties.

Consistent with other similar authorities, the regime should require regular briefings, consultations and updates to congressional committees of jurisdiction at periodic intervals on

general trends in Commerce's use of emergency authorities. These briefings should not include confidential business information and be classified if necessary.

In addition, Commerce should impose explicit limits on and clear standards to guide the Secretary's discretion to provide notice to the parties of its review of a transaction "when consistent with national security." Commerce should moreover establish a process for providing notice, including the factual basis for the action, and an opportunity to be heard in situations in which advance notice is withheld.

d. Identify "foreign adversaries" with specificity to facilitate predictability, compliance and deterrence.

The modified Proposed Rule should establish a set of public criteria to guide a fact-based analysis about how to define a foreign adversary, with priority focus on specific entities or persons rather than whole countries. Moreover, Commerce should specifically identify the entities that are designated as foreign adversaries and state what restrictions apply to such entities. This approach would allow for identification of foreign adversaries to give U.S. businesses and persons notice to inform their business planning and activities (i.e., similar to screening for parties on Office of Foreign Assets Control or Bureau of Industry and Security restricted party lists) and also facilitate compliance and deterrence to advance the underlying national security objectives.

e. Share threat and vulnerability assessments and provide the essential reasoning in summaries of final determinations.

To provide clarity on the scope of this new regulatory regime, the threat and vulnerability assessments Commerce will rely upon should be declassified and made available to private-sector stakeholders to the greatest extent possible. If classified or highly sensitive, they should be shared with appropriate stakeholders that hold the necessary security clearances.

As directed by the Executive Order, the Department of Homeland Security should establish a recurring, transparent and inclusive process for producing and updating an assessment that identifies entities, hardware, software and services to help inform stakeholders. Commerce should also establish a process to solicit specific and constructive feedback from industry on how the specific concerns can be addressed without overburdening industry with unnecessary uncertainty.

To further promote transparency, Commerce should publish — in unclassified form to the greatest extent possible — high-level descriptions of reviewed transactions, the national security threat identified in those transactions and the ultimate action taken by Commerce. These descriptions should not disclose confidential business information or the names of parties to the transactions.

f. Refine the criteria to assess a transaction.

With respect to Proposed Rule § 7.101(a)(5), Commerce should remove the reference to the "digital economy" as this term is vague and could be read as all encompassing. Instead, Commerce should better define what constitutes "critical infrastructure" for the purposes of this framework and thereby capture the aspects of the digital economy where the identified vulnerabilities exist. Commerce should also revise Sections (i) and (ii) to state "unacceptable risk" (instead of "undue risk"), consistent with (iii) in setting a common standard for all three criteria.

g. Amend the review process.

Commerce should grant *de facto* approval for a transaction if the Secretary does not reach (1) an initial determination within 30 days of commencing a review or (2) a final determination within 30 days of a company filing documentation in opposition to an initial determination. As the Proposed Rule currently provides the Secretary with discretion to extend the timeline for review, establishing clear expectations for consideration would reduce uncertainty for parties by ensuring that a review could not continue indefinitely. Alternatively, the Secretary's discretion to extend the timeline for review should be subject to a specific time limit and should be exercised only in extraordinary circumstances, as assessed by reference to specific factors or criteria.

In addition, there should be a formal, interagency appeals process. Such a process, which would be consistent with similar regimes (e.g., export controls and CFIUS), would increase transparency and accountability for the new regulatory regime and ensure a more holistic interagency approach.

h. Establish clear criteria for the use of information from foreign governments and private parties.

The Proposed Rule does not define the parameters of what types of information provided by a foreign government or private party can be used as the basis for a transaction review other than that information provided by a private party must be "credible." To prevent anti-competitive behavior or abuse under this framework Commerce should use only information from foreign governments and private parties that Commerce can independently corroborate. In addition, if a private party's submission of information triggers the review of a transaction, that information should be duly provided to the entity subject to the review so that it has the opportunity to respond to what may be inaccurate or false information.

i. Provide additional protections to confidential information.

To encourage parties to better cooperate with Commerce during a review, Commerce should withhold and protect from disclosure, to the fullest extent permitted by law, any confidential business information submitted to it during the review process.

###

Business Roundtable recognizes the importance of securing U.S. ICTS supply chains to protect national security. The critical nature of the ICTS sector to U.S. national security and economic prosperity warrants additional and ongoing consultation and cooperation with the private sector to achieve shared goals of protecting national security and increasing U.S. economic growth and competitiveness. We recommend that Commerce and the Administration work closely with industry and the private sector to rework the Proposed Rule and issue a second Proposed Rule for notice and comment before issuing a final rule.

Thank you for consideration of these comments. Business Roundtable appreciates the opportunity to continue engagement with the Administration on its ICTS supply chain efforts.