ITI Promoting Innovation Worldwide

March 22, 2021

Mr. Henry Young
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

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

Dear Mr. Young:

The Information Technology Industry Council (ITI) appreciates the opportunity to continue its engagement with the Department of Commerce ("Commerce") as it develops the rule to implement Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain* via additional comments on the Interim Final Rule (hereinafter the "IFR" or "rule").

The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies. Founded in 1916, ITI is an international trade association with a team of professionals on four continents. We promote public policies and industry standards that advance competition and innovation worldwide. Our diverse membership and expert staff provide policymakers the broadest perspective and thought leadership from technology, hardware, software, services, manufacturing and related industries.

Most of ITI's members service the global market via complex supply chains in which technology is developed, made, and assembled in multiple countries, and service customers across all levels of government and the full range of global industry sectors, such as financial services, healthcare, and energy. We thus acutely understand the importance of securing global ICT supply chains as not only a global business imperative for companies and customers alike, but as critical to our collective security. As a result, our industries have devoted significant resources, including expertise, initiative, and investment in cybersecurity and supply chain risk management efforts to create a more secure and resilient Internet ecosystem.

Of paramount importance to ITI and its member companies is our shared commitment to address risks to global information and communications technology supply chains and national security more broadly. We believe government and industry must work together to achieve the trusted, secure, and reliable global supply chain that is essential for protecting national security and an indispensable foundation for supporting innovation and economic growth.

We appreciate that Commerce has attempted to inject more certainty into this rulemaking by providing clarification and detail on certain items we had originally raised concerns with. However, the rule remains too broad and indefinitely retroactive to be practically implementable. Further, its breadth will undermine the supply chain and national security objectives it purports to address. ITI is concerned about the almost limitless discretion granted to the Secretary of Commerce ("the Secretary") over such a large portion of the ICT sector. It is not clear to us whether this is something

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

that is fixable in a final rule, given the underlying Executive Order on which this rulemaking rests is problematic in its overbroad scope. At a minimum, ITI recommends that Commerce delay implementation of the IFR while comments from stakeholders are reviewed.

Given Commerce has been charged with co-leading a holistic assessment of the ICT supply chain as called for by the new *Executive Order on America's Supply Chains* (EO 14017), we believe it is appropriate to take a fresh look at the authorities granted by the ICTS EO as well as the early implementation of these authorities pursuant to this IFR. Indeed, we strongly encourage the Biden Administration to undertake a strategic review of ICT supply chain security policy as part of the assessment called for by the new EO to develop a more coherent, streamlined and effective long-term strategy, including delaying further implementation of the rule in whole or part as appropriate pending that required broader assessment. In doing so, the Administration should consider how to address legitimate national security issues in a *coordinated*, *holistic,* and targeted manner. We elaborate on these ideas in our recently released Supply Chain Security Principles.[1] Measures that create a new regulatory regime that inject uncertainty and new risk into the essential ICT sector must be weighed against the benefit to security, a test which the ICTS EO and the IFR seem to fail.

It is through this lens that we offer our comments in response to the IFR, which primarily focus on the following: (I) overarching concerns with the IFR; (II) comments on the IFR; and (III) recommendations for improved implementation of the IFR.

I. Overarching Concerns with the IFR

Although our comments are intended to provide constructive advice, we continue to believe that the IFR is fundamentally flawed in several respects. In order for this rule to be at all workable while upholding American national security, U.S. economic competitiveness, and overall due process, several areas need to be thoroughly clarified or reconsidered. Immediately below we offer several overarching comments in this regard.

The scope and breadth of this rule remains impossibly broad and raises significant due process concerns. The IFR remains too broad to be practically implementable and goes well beyond that which is necessary to protect national security and prevent undue security risks to critical infrastructure supply chains. As a result, the IFR continues to cast a cloud of uncertainty over substantively all ICTS transactions with any nexus to the United States, including those that present no or low risks to national security. While we are encouraged that Commerce has attempted to take a risk-informed, technology-neutral, case-by-case approach grounded in specific, factual information, including as it relates to potential mitigations, the scope of the IFR as currently drafted is far too vague, overbroad, and replete with unknowns for our member companies to meaningfully understand how they would practically comply with such a regime. As such, the IFR provides inadequate notice and raises significant concerns regarding due process and fairness which must be remedied in further iterations of the Rule.

The IFR continues to create uncertainty for businesses, serving to undermine the competitiveness and technological leadership of U.S. companies during a time of turmoil for the U.S. economy. While Commerce has attempted to provide further clarity in some areas, on the whole, the scope of the rule coupled with the broad discretion granted to the Secretary continues to make for an

[1] https://www.itic.org/policy/ITI_SupplyChain_Principles2021.pdf

uncertain business environment and threatens the ability of U.S. companies to compete with foreign companies not subject to similar conditions. The ICTS EO was originally published in May 2019, a time when both the U.S. economy and U.S. citizens were stronger and healthier. The ICTS EO did not anticipate the severe strains and challenges of the past year, driven in large part by the global pandemic. Overbroad policy approaches, such as those which continue to be embodied in the IFR, stifle U.S. innovation, technological leadership, and competitiveness and do not serve to further national security. The potential retroactive effect of the rule is particularly troubling for U.S. companies as it takes time to unwind or adjust supply chain relationships with significant costs. Commerce and other U.S. policymakers should seize the opportunity to advance supply chain policy approaches that are not only compatible with but drive global policymaking norms.

To expedite America's economic recovery in the wake of COVID, Commerce should avoid measures that impede innovation and undermine U.S. global competitiveness and instead invest in it. Especially as the U.S. economy emerges from the turmoil of the past year's global pandemic, U.S. global competitiveness and commercial success – both of which are critical to U.S. national security – depend upon regulatory certainty and clarity. However, the IFR fails to deliver this certainty, as it continues to capture huge swaths of ICTS in its scope and grants vast discretion to the Secretary to block or restrict commercial transactions of US companies. Casting an overly wide net to secure America's ICTS supply chain in the form of import restrictions as contemplated under this IFR could inhibit the development and commercialization of new technologies in the United States, therefore undermining U.S. technological leadership and competitiveness by driving R&D programs and business "transactions" to jurisdictions that do not impose such constraints. It could also restrict U.S. firms' and researchers' access to the ICT products and services that are critical to advancing R&D.

Commerce's own Regulatory Impact Analysis estimates that the IFR could impact 268,000 to 4,533,000 firms and compliance could cost them $210 million to $20 billion. Many of these companies are already strained by severe supply chain disruptions from the pandemic to semiconductor shortages. Additionally, the IT sector responded successfully during the past year's global pandemic, leveraging its global supply chains to continue providing semiconductors, cloud services, communication services, networking technology, security solutions, data centers and many other types of technology to allow millions of Americans to remain productive and allowing America's employers to keep high paying jobs. The creation of a new, large scale regulatory regime governing ICT supply chains just as the U.S. may be emerging from the pandemic turmoil is counter-productive and will weaken the U.S. economy's recovery.

The process for developing and implementing the Rule has been confusing. The normal steps which industry expected Commerce might follow to robustly develop and implement this rulemaking have seemingly been ignored throughout the process of the Rule's development, which has further contributed to the uncertainty surrounding the rule. For example, the Rule will become effective with no voluntary mechanism in place to help companies understand what transactions might fall within scope and such a mechanism won't be developed until 60 days after the Rule becomes effective.

The business community is an indispensable partner to Commerce in any efforts to effectively implement this rulemaking. ITI appreciates Commerce's decision to seek additional comment on this IFR, as doing so allows the business community to provide critical feedback to Commerce as it seeks to tailor the implementing measures to the national security imperatives underlying Executive Order 18373. We encourage Commerce to continue to engage with industry as Commerce seeks to

implement the rulemaking considers establishing a voluntary licensing process. In every case, we urge Commerce to consult with industry as early in the process as possible.

II. Comments on the IFR

A. Definitions

The Executive Order grants the Secretary the authority to prohibit any acquisition, importation, transfer, installation, dealing in, or use of (a "transaction") information and communications technology or service subject to US jurisdiction. Although we had encouraged Commerce to provide additional clarity around key terms and definitions in response to the NPRM, including the terms "ICTS" and "transaction," among others, the IFR unfortunately does not provide necessary clarity on these and many other key terms. We continue to encourage Commerce to more narrowly define these terms.

Interest: Commerce does not further define "an interest" in the IFR. We continue to urge Commerce to further define what "an interest" means with regards to "property in which any foreign country or national thereof has an interest." The language remains overbroad and would capture transactions in which a foreign person has only a tangential, non-controlling interest. To align with national security objectives, Commerce should revise this definition to only apply where there is a nexus to a "foreign adversary." At a minimum, an exclusion should be provided for de minimis interests, such as a bank financing an entity through a letter of credit or minority or non-controlling interests. This would focus the definition of "an interest" narrowly and clarify the intent as to capture majority or controlling interests at the time of the transaction.

Foreign adversary: Although Commerce has added a specific section that identifies foreign adversaries for the purposes of the Executive Order, we remain concerned about casting an entire country as in scope, particularly given the broader impact of the definition on the operations of U.S.-based companies and their employees who may be subject to the jurisdiction of the laws of such foreign adversaries, such as subsidiaries of U.S. firms and those of our allies. For example, the current definition of "foreign adversary" would extend to include any individual employee of a U.S. company who is a citizen of China or Hong Kong (including H-1B and green card employees in the United States); taken together with the broad designation of "transaction" (discussed below), the IFR would seem to require a novel regulatory structure in which ICT companies must classify certain employees, based on citizenship, as foreign adversaries, whose every contribution to technology development, technical support, or sales is subject to this new regulatory review. We recommend, at a minimum, further clarifying the definitional scope of "foreign adversaries" to exempt employees of U.S. companies who are citizens of covered countries and explain which companies are intended to be captured, and which are not.

Transaction: We previously urged Commerce to further define "transaction." Unfortunately, the IFR does not provide additional clarity and relies upon the same definition as is used in the Executive Order, ostensibly capturing every activity undertaken by a company – in other words, the constant motion of companies' business activities. The term "transactions" and each of the illustrative terms comprising the definition itself must be clearly elucidated in a manner that helps to clarify the national security imperative at the core of the EO and IFR and enable companies to comply. By clarifying these terms, companies would have notice of the *types* of commercial activity that may be subject to additional scrutiny and those that are not, thus minimizing regulatory burdens, delays, and

costs and reducing the need to seek additional guidance from Commerce for specific transactions, which will only put more burdens on its staff.

One approach to defining what elements of "transactions" are covered would be to eliminate the illustrative terms that are either redundant with the term "transaction" itself or that are so vague as to only introduce confusion – such as "dealing in" and "use." This approach to defining "transactions" would seem to extend to many business activities that are essential to the operation of a modern, global firm. For example, the IFR would seem to extend to a firm's internal transfer of a software module from a development team in a covered country to a validation team in the U.S. Instead, Commerce should clearly articulate what commercial activities are not intended to be captured. For example, broad terms such as "dealing in" clearly capture all manner of transactions, including export and investment transactions that are likely covered under other regimes. We recommend Commerce carefully delineate which transactions cannot be considered in scope by employing an approach that embraces principles of statutory interpretation and by examining the impacts of such a broad definition on U.S. competitiveness consistent with the broader review and assessment required by the America's Supply Chains EO.

We continue to recommend additional clarification by precisely defining the other terms that can trigger the prohibition of a transaction – "acquisition," "importation," "transfer," and "installation." To the extent such terms are defined by other regulatory frameworks, we recommend incorporating or referencing such definitions. We also recommend further clarifying these terms as limited to covering transactions that are clearly subject to U.S. jurisdiction and not covered by other national security review mechanisms. For example, export transactions should be out of scope because they are already regulated by the export control regime via the Export Administration Regulations (EAR). Likewise, investment transactions should be considered as out of scope because they are regulated by CFIUS, etc.

Jurisdiction: While we appreciate that Commerce has attempted to lend additional clarity to the term "jurisdiction" by adding a definition of a "person owned by, controlled by, or subject to the jurisdiction of a foreign adversary," the definition remains problematically broad. The defining language ("any person, wherever located, who is a citizen or non-resident of a nation-state controlled by a foreign adversary; any organization organized under the laws of a nation-state controlled by a foreign adversary)" will extend to large numbers of employees of companies based in the U.S. and allied countries, employees who are vital to the successful operation of a modern global technology firm. It also would cover U.S. citizen employees who might be based in covered countries. "Jurisdiction" as defined still serves to capture a broad swath of activities with no significant nexus to U.S. national security interests.

Sensitive personal data: The IFR adds a new, very broad definition of "sensitive personal data." This definition is troubling and goes beyond what is considered to be "sensitive personal data" in other data protection laws and best practices, such as the GDPR. In addition, collecting and retaining data for over a million people over a 12-month period is common for many multinational companies, and oftentimes such practice does not create issues with sensitivity. We therefore recommend that Commerce further narrow the definition of sensitive personal data and align with international best practices.

B. Retroactivity

The IFR includes a provision on retroactivity. Section 7.3. states that although the rule will not apply to ICTS transactions initiated, pending, or completed before January 19, 2021, the rule applies to software updates deployed after January 19, 2021, even if the update is pursuant to an agreement executed prior to January 19, 2021. This aspect of the IFR provides it with indefinite retroactivity – Commerce could initiate a review of a transaction that is one, three, or five years old simply because of when a software update is issued. This generates significant uncertainty for broad swaths of industry, particularly given that providing security updates is a widespread security best practice.

The rule should not have retroactive applicability to materials and services that are in "use" today. The greatest challenge to companies in complying with this rule is the difficulty in forecasting what transactions Commerce will consider as within scope. Without being able to predict what transactions will fall under the rule, companies cannot build compliance into their supply chains and infrastructures to prevent the risks that the rule is intended to thwart. Rather, the rule takes a retroactive approach in penalizing companies for a broad set of transactions that may be later found to be risky.

C. Evaluation Process & Criteria

We appreciate that the IFR attempts to provide additional clarity regarding the process by which the Secretary will evaluate a transaction. However, it is our view that the IFR falls short in providing the clarity required to grant an adequate level of certainty to businesses.

1) Initiating the review of a transaction, including first and second consultations with the interagency

The process by which the Secretary will initiate a review of a transaction, including to consult with other agency heads to determine whether a transaction should be evaluated, lacks clear parameters.

The interagency consultative process, in particular, remains vague. Despite offering additional detail about when the Secretary will engage with other agency heads throughout the evaluation process, the IFR does not establish a formal consultative process for doing so. Businesses are left to wonder whether this will include an ad-hoc engagement every time a potential transaction falls within the scope of this authority or whether a more formal process will be employed.

We recommend establishing a formal interagency vetting process to evaluate transactions, requiring all agencies to provide input on key decisions regarding whether a transaction is a) in scope and b) presents a national security risk to the United States that is not addressed by other means. We recommend Commerce first look to existing interagency bodies and review processes that are well-established in existing statutes as examples that could serve as a model, such as CFIUS, and establish a similar, formal interagency group here.

We appreciate that Commerce has attempted to provide additional clarity around how the Secretary can launch a review of a transaction. Although the IFR appears to do away with the notion that the Secretary can launch a review based on information received from private parties, the fact that the Secretary has the discretion to deem information as relevant or credible is still troubling. Further, because the IFR grants the Secretary the ability to launch a review at his/her discretion, we remain concerned with the seemingly boundless nature of this authority as it continues to cast a shadow of uncertainty over nearly all ICTS transactions. A formal interagency process, including convening a

session or establishing consensus on whether a transaction is subject to the Rule, as outlined above, would provide a holistic government view, as would be appropriate where the government is weighing whether to intervene in dealings between private parties.

2) Scope of covered ICTS transactions

The scope of ICTS transactions captured by the IFR is all-encompassing and appears to be even broader than the criteria laid out in the Executive Order. The Executive Order prohibits transactions that a) involve ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary and b) pose an undue risk of sabotage or subversion to ICTS in the U.S., or pose an undue risk of catastrophic effects on the critical infrastructure or the digital economy, or otherwise pose an unacceptable risk to national security.[2]

By contrast, Section 7.3(a) of the Rule provides that the transaction may be subject to evaluation if it is: (1) conducted by U.S. persons or involves property subject to U.S. jurisdiction; (2) involves any property in which a foreign country or national has an interest; and (3) was initiated or completed after January 19, 2021; (4) involves any of the ICTS designated in the IFR.

Without further guidance, it appears that almost every U.S. technology transaction involving an international business partner, even involving a single employee based in the U.S. who is also a citizen of a covered country, could trigger a review under this Rule. This seemingly extends to transactions that do not create any risks at all. As noted above, including review of all transactions where there is simply a "foreign interest" is overbroad. We urge Commerce to avoid considering all foreign transactions as potentially in scope, but rather only those that involve a specific, identified risk, as all foreign transactions are not inherently risky. At a minimum, the current broad scope could impose a burden on Commerce that jeopardizes its ability to focus its limited resources on the transactions that are most likely to raise national security concerns.

We also urge Commerce to clearly articulate the criteria that are used to assess the "effect" of a particular transaction, which in our view should be clearly related to the actual national security risk posed by the transaction. As such, these criteria should be focused on addressing acute and clearly articulated national security risks to the United States and should not include trade policy or other commercial concerns.

The IFR is not clear as to whether the ICTS transaction definition includes use of information in the public domain without the exchange of payment between the parties. Transactions of this nature are generally not tracked by U.S. companies and the rule should not require U.S. companies to build the muscle to police such transactions. Additionally, non-commercial transactions (e.g., transactions made for charitable or donative purposes) may necessarily involve incurred costs by the donor that are not recoverable. Because of the relative level of investment that is required, the definition's potential application to free or no cost transactions involving information in the public domain could have an outsized stifling effect on these types of critical transactions relative to other transactions. In addition, subjecting free or no cost updates or repairs necessary for the security of ICTS on commercial transactions or uses that are not necessarily in the public domain to a review process is counter to the underlying national security objectives. We therefore strongly recommend that

[2] Executive Order 13873, 84 FR 22689 (May 15, 2019).

Commerce clarify the ICTS transactions definition to explicitly exclude information in the public domain as well as no cost updates and repairs.

Finally, in our previous comments on the NPRM, we recommended that Commerce delete the phrase "subject to the jurisdiction of." We continue to recommend that this term be narrowed or deleted entirely, as keeping this language drastically expands the scope of entities that would be captured by this rule. Indeed, any company operating in a nation considered to *be a* foreign adversary, including a subsidiary of a U.S. company, would be subject to the laws (and hence jurisdiction) of that country. Therefore, being subject to the jurisdiction of a country designated as a foreign adversary is overbroad and should not be a decisive factor in triggering a review, as it is a potentially meaningless designation in the context of companies doing business globally. It would also put massive burdens on Commerce, whose resources can best be targeted to specific transactions that involve serious national security risks, as opposed to being spread across countless ordinary business transactions.

3) Notifying parties & issuing determinations

In our comments to the NPRM, we stressed the importance of transparency and due process in providing businesses with certainty, therefore allowing for improved competitiveness. We appreciate that the IFR provides significant additional clarity on how the Secretary will notify parties and issue determinations, including providing additional protections for business confidential information received during the review process. However, we still have concerns with certain aspects of the process as outlined in the rule.

First, the rule specifies that an initial determination may be published in the Federal Register "where the Secretary determines that the initial determination concerns or could impact entities beyond the parties to the ICTS transaction." While it would be helpful for Commerce to publicly provide some information regarding the types of transactions it has reviewed and the results, further public disclosure of the names of involved parties could cause substantial economic and reputational harm to U.S. businesses, even where mitigation mechanisms are available and have been employed to address any perceived risks. Thus, we urge Commerce only to publish information that would not directly or indirectly reveal the names or identities of the parties to the transactions. By way of example, we note that CFIUS generally does not publish detailed information regarding the parties or transactions that it reviews.

We had also recommended in our initial set of comments to the NPRM that Commerce allow for a 60-day post-notification response period for parties to respond to any initial determination related to a transaction, including assembling the appropriate information and/or establishing appropriate mechanisms to mitigate any identified risks related to that transaction. However, the IFR maintains a 30-day response period, which we continue to believe is too short. Commerce's process for stakeholders to appeal a denial of an export license application under the EAR offers a potential model to consider, whereby Commerce provides for a response window of 65 days, including three opportunities to respond to and appeal the process, which allows for a more collaborative approach with the agency.[3]

[3] See 15 C.F.R. § 750.6(b).

III. Recommendations for Improved Implementation

The Biden Administration's efforts to initiate targeted reviews of critical supply chains in Executive Order 14017 represent a much more constructive approach to engaging agencies and industry to jointly identify problems and opportunities. We recognize that the IFR was published in the closing hours of the prior Administration. Below, we offer specific recommendations to address the many shortcomings of the IFR. These would have to be addressed if the IFR is to be reconstituted into workable policy.

A. Narrowing the scope

In our response to the NPRM, we urged Commerce to dramatically narrow and significantly clarify the scope of transactions covered by the rule. While we appreciate that Commerce has attempted to narrow the scope by designating specific foreign adversaries and listing out particular classes of technologies that will definitely be subject to the rulemaking, the scope remains problematically broad and as drafted will still capture wide swaths of transactions that do not pose a risk to national security.

Although Commerce has listed classes of technologies that will be subject to the rulemaking in the IFR, when taken as a whole, the list is so wide-ranging as to be practically useless with respect to providing any sense of boundaries of coverage. It includes most transactions in the ICT sector, including many transfers of products and technology within a single multinational company. It also includes products "that process personal data of over one million US persons" without any specific link to a national security risk associated with such data processing. The list also captures any ICT technology used in critical infrastructure sectors designated by PPD 21 as well as "any ICTS technologies integral to AI and machine learning, quantum key distribution, quantum computing, drones, autonomous systems, or advanced robotics," among many others. There are no ICTS transactions that are categorically excluded. While we agree that categorical exclusions of entire classes of technologies run counter to a case-by-case approach, we also believe that in order for this rulemaking to be implementable, transactions that lack a nexus to a specific threat or vulnerability articulated in U.S. government intelligence or vulnerability assessments need to be excluded. The EO required that ODNI undertake a threat assessment of potential foreign adversaries, and additionally directed DHS/CISA to conduct a review of the risks/threats posed by ICTS products/services to help determine what should fall into scope.[4]

While the initial DHS/CISA criticality assessment represents an assessment of ICT products and services at a particular moment in time, we encourage Commerce to rely upon the methodology developed by DHS/CISA and to conduct an update of this criticality assessment in consultation with the private sector to help further narrow the IFR's scope. Factors developed by CISA and used to conduct the initial criticality assessment included identifying: how important an ICTS element is to the operation of the function the ICTS supports; the importance of the confidentiality, integrity, and availability of the information flowing over the ICTS element; the importance of the function the ICTS element supports; and what damage the ICTS element could cause to national security if compromised. We recommend that CISA continue to evolve its methodology for assessments of ICTS in the future and suggest that they consistently review and update the initial list of critical ICTS elements. CISA may then use this assessment process to conduct periodic reviews and ensure it

[4] https://www.cisa.gov/publication/ict-eo-13873-response

continues to remain up to date, to best address currently understood risks to ICTS. The CISA-led ICT SCRM Task Force additionally developed a comprehensive threat evaluation of ICTS which should also be leveraged by Commerce to help narrow the scope of ICTS transactions giving rise to risks that rise to the threshold of needing to be reviewed pursuant to the rule.

We had previously recommended a series of steps Commerce could take to narrow the scope, including:

- **Categorically excluding transactions that lacked a specific nexus to a clearly identified national security threat**. If a transaction does not implicate a specific, identified threat or vulnerability articulated in U.S. government intelligence or vulnerability assessments, it should not be covered by the rule.
- **Developing a list of mitigating/aggravating factors to help Commerce identify whether a transaction is more or less likely to present a risk to national security**. Examples of categories that may be inherently low risk and thus should be considered as candidates for exclusion include: (1) mass market electronic devices primarily intended for home or small office use; or (2) commercial off-the-shelf (COTS) items that do not require modification or maintenance over their lifecycle. We note that the IFR says that personal ICTS hardware devices, like handsets, "do not warrant particular scrutiny." Commerce should narrow the scope by definitively listing out additional categories that do not warrant particular scrutiny and therefore, do not fall under the umbrella of this rule.
- **Adopting the same exclusions as are adopted for Section 889** of the John S. McCain National Defense Authorization Act for FY 2019 ("FY 2019 NDAA"): (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.
- **Focusing on ICTS entering the US, not on exports.** As noted above, the ICTS Rule should not apply if other existing U.S. legal authorities are available. However, the rulemaking does not make clear whether exports are in scope of the ICTS rule, despite the fact that the existing EAR and corresponding export control regime already perform this function for Commerce. Therefore, the Rule should clarify that export transactions are out of scope.
- **Limit to future transactions.** The rule should be limited to transactions pending or completed on a date six months after the date the final rule is issued. This would provide certainty to industry that pre-existing transactions would not be subject to sudden review years after they had been executed. The six-month implementation date would give businesses time to ensure that they take into consideration the new rule when engaging with potential business partners.
- **Further define "transaction," including providing greater specificity as to the types of transactions that present an undue risk to national security**. For example, the EAR clearly defines what is and what is not an "export" subject to the export control regulations, while CFIUS likewise provides specific information as to the types of transactions that fall under its purview. Similar to CFIUS, Commerce should also provide illustrative examples of what is covered and what is not, and provide an opportunity to comment on those examples, to ensure that they effectively capture transactions that pose national security risks. These approaches allow businesses to clearly understand what is required to comply with these regimes – an element that is clearly missing from the ICTS rule.

We reiterate here these recommendations, which we believe would be immensely helpful to further scoping this rulemaking.

B. Clearly articulate evaluation criteria, including determining undue or unacceptable risk

While we appreciate that the IFR outlines information sources that the Secretary and agency heads may rely upon when determining whether a transaction poses an "undue" or "unacceptable" risk, the criteria for what constitutes such a risk are not well-defined. The IFR references the definition of "undue" or "unacceptable" risk used in the Executive Order, which is vague and thus provides limited information as to *what* transactions the Secretary might deem to pose such a risk. It also grants the agency wide discretion to make judgment calls as to risk determinations and leaves U.S. companies in the dark as to what is covered.

Although we appreciate that the IFR lays out at least some criteria that the Secretary may consider when determining whether a transaction poses an undue or unacceptable risk in part 7.103, we encourage Commerce to also consider whether a compromise in the availability, confidentiality, or integrity of a particular product or service would impact an important national interest. The vast majority of products and services would not affect a national interest and would not constitute an undue or unacceptable risk.

We also urge Commerce to provide additional information on the criteria it used to determine foreign adversaries for the purposes of this rule. As it stands, these foreign adversaries were seemingly determined in a vacuum based on "threat assessments and reports from the U.S. Intelligence Community, the U.S. Departments of Justice, State, and Homeland Security, and other relevant sources." and without an understandable, repeatable process in place. As such, it is not clear whether or how a new country could be added to the list, again contributing to an uncertain business environment in which transactions could suddenly come under review if a new country is unexpectedly added to the list.

C. Issue advisory opinions

We continue to urge Commerce to consider a mechanism allowing for advisory opinions to be issued regarding specific transactions that companies may be contemplating. This would provide concrete guidance to businesses seeking to comply with the EO. As written, the rule is so broad it is difficult for businesses to know how to undertake transactions so as to comply with the rulemaking outside of not doing business at all with entities with a nexus to China, Russia, or other designated foreign adversaries. Ultimately, guidance that could be applied more broadly and that would help businesses avoid high-risk transactions would reduce national security risk more effectively. ITI would be open to discussing with Commerce the format that such an advisory opinion or guidance process might take.

D. Avoid duplicative review processes

Although we appreciate that the IFR excludes review of transactions that have undergone or are currently undergoing CFIUS review, and indicates that the intent of the rule is to be "complementary" to other existing measures, it does not go far enough to demonstrate *how* it would avoid duplicating efforts with mechanisms already in place such as the EAR, International Traffic in Arms Regulations (ITAR), CFIUS, relevant provisions of the FY 2019 NDAA (including Section 889, FIRRMA, and ECRA),

relevant provisions of the SECURE Technology Act; the recent FCC restriction on certain telecommunications equipment in U.S. 5G networks, and Team Telecom processes. Additionally, this exclusion will only have a slight impact on narrowing the number of transactions subject to review. It is unlikely to insulate from ICTS review the vast majority of ICTS Transactions and therefore offers limited predictability for the private sector. The CFIUS review process encompasses only foreign *investment* in U.S. business, so the present CFIUS exclusion will not necessarily provide any predictability about the large number of transactions involving the acquisition, importation, transfer, installation, dealing in, or use of any ICTS subject to review under the IFR.

Below, we lay out recommendations for further excluding transactions from review that have already been subject to governmental scrutiny for national security concerns:

- **Include a limiting principle for the use of this authority.** ITI previously recommended that Commerce include a limiting principle for the use of this authority, similar to CFIUS: if other legal authorities exist to mitigate and/or address an identified national security risk, this rule should not apply. For example, CFIUS operates under a statutory and regulatory rule that its authorities apply only when the government's national security concerns are not adequately addressed through other laws and regulations.[5] However, a limiting principle was not included in the IFR; only a nod to CIFUS. We urge Commerce to more clearly include a limiting principle to avoid the potential for a transaction to be captured under multiple review processes.
- **Exclude transactions under active review or previously reviewed by the *Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector* (Committee).** This Committee is made up of Executive Branch agencies that "assist the [Federal Communications Commission (FCC)] in its public interest review of national security and law enforcement concerns that may be raised by foreign participation in the United States telecommunications services sector."[6] In this review, the Committee evaluates applicant businesses' ownership, operations, personnel and management, principal equipment in systems and networks, data handling practices, and more. Dozens of questions are posed covering, for example, compliance with regulations from more than a dozen U.S. regulators, as well as comparable state and foreign agencies. The Committee frequently

[5] *See, e.g.*, 50 U.S.C. § 4565 note ("The Committee, or any lead agency acting on behalf of the Committee, may seek to mitigate any national security risk posed by a transaction that is not adequately addressed by other provisions of law" (incorporating Exec. Order 11858, sec. 7)); *id*. § 4565(d)(4)(B) ("The President may exercise the authority conferred by paragraph (1), only if the President finds that … provisions of law, other than this section and the International Emergency Economic Powers Act [50 U.S.C. 1701 et seq.], do not, in the judgment of the President, provide adequate and appropriate authority for the President to protect the national security in the matter"); 31 C.F.R. § 800.101 ("The principal purpose of section 721 is to authorize the President to suspend or prohibit any covered transaction … when provisions of law other than section 721 and [IEEPA], do not, in the judgment of the President, provide adequate and appropriate authority for the President to protect the national security in the matter before the President."); *id.* § 800.501(a) ("The Committee's review or investigation (if necessary) shall examine, as appropriate, whether … [p]rovisions of law, other than section 721 and [IEEPA], provide adequate and appropriate authority to protect the national security of the United States.").

[6] The FCC refers certain applications that have reportable foreign ownership to the Department of Defense, Department of Homeland Security, Department of Justice, Department of State, U.S. Trade Representative, and Department of Commerce's National Telecommunications & Information Administration (NTIA) for their review. *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, Report and Order, 35 FCC Rcd 10927, ¶ 3 (2020).

negotiates commitments from companies which are designed to protect supply chain security, such as requiring disclosure and Committee approval of principal equipment and certain service providers as well as prohibitions designed to address network security. Accordingly, it would be logical to exclude transactions involving companies that have undergone Committee review from the ICTS review process because their supply chains have already been scrutinized.

- **Exclude transactions with parties that have been vetted for national security risks.** Commerce should take additional steps to clarify the rule's applicability and reduce burdensome and duplicative reviews that may tax Department resources for no appreciable security benefits. For example, Commerce can not only exempt *transactions* that have already undergone CFIUS or Team Telecom review, but it should also exempt the *foreign parties* who were the applicants subject to CFIUS or Committee review. If CFIUS or the Committee and the FCC have found that ownership or control by a foreign company does not raise national security concerns, then it follows that commercial ICTS equipment or services transactions with the same company should not raise concerns. Commerce should exclude from its review ICTS transactions between U.S. companies and parties that have already been approved by federal agencies.

E. Evaluation criteria should not rely solely on designation of covered countries

The IFR appears to rely almost exclusively on its designation of covered countries as deterministic of risk, which may result in the inclusion of many entities that pose no appreciable risks to national security or critical infrastructure and serves to potentially exempt entities from review who could pose such risks. Country of origin is only one factor that should be considered in assessing the risks related to ICTS transactions – the overriding purpose of the evaluation process that is the subject of the Rule – and should not be conflated with the evaluation of threats related to countries so designated (which was the purpose of the ODNI assessment required by the EO). Modern practice of supply chain risk management comprehends many factors in evaluating the trustworthiness of potential suppliers. ICT companies have led American business innovation in managing risk in global supply chains to mitigate sources of risk which may include country of origin for specific technologies, hiring and employee management practices, ensuring multiple sources for critical goods, building robust and ongoing monitoring systems and investing in trusted logistics systems.

F. Establishing a voluntary licensing process

Should the Administration keep the IFR in place, we are pleased to see that Commerce intends to develop a voluntary licensing process associated with this rulemaking and encourage the agency to follow through in developing such a mechanism. Such a process will allow for more certainty in the business community and will also provide the government more insight into the proposed transaction while also ensuring that the parties to the transaction understand what national security bounding conditions will apply in a given set of circumstances. However, we are concerned with the fact that the licensing process is not due to be published until 60 days after the Rulemaking becomes effective, leaving a significant gap during which it will be difficult for companies to have any level of certainty surrounding their transactions. That being said, the scope of the IFR as drafted will likely result in an overwhelming amount of pre-clearance/licensing requests, and so we encourage Commerce to think through this as they continue to discern how to implement this rulemaking. An effective licensing or pre-clearance process will require significant staffing and funding.

In its efforts to establish a voluntary licensing process, we recommend Commerce provide specific guidance on what types of transactions should be submitted for a license and which should be more appropriately subject to mitigation measures, which could help provide clarity on what the rule is trying to get at in the first instance and help cut down on unnecessary license applications. As a part of this effort, we encourage Commerce to obtain stakeholder feedback on the licensing process, including making it available for public comment so as to ensure it is structured as effectively and efficiently as possible.

G. Identify and designate a specific bureau/agency within Commerce to lead the implementation of this rulemaking

It is not clear what bureau or agency within Commerce will be responsible for carrying out this rulemaking, including receiving, reviewing, and responding to voluntary licensing requests. We urge Commerce to identify a lead agency or bureau to coordinate the implementation of this Rule. In doing so, we urge Commerce to include a request that the agency or bureau designated as lead in implementing this rule is appropriately resourced and funded in the budget it submits to the White House OMB.

***

ITI appreciates the opportunity to submit comments in response to the IFR. As stated above, we believe industry and government must work together to achieve the trusted, secure, and reliable global supply chain that is a necessary priority for protecting national security and an indispensable building block for supporting innovation and economic growth. Working together to develop a narrowly tailored and focused rule will help to achieve the shared objective of strengthening our collective security without harming U.S. technological leadership and competitiveness.

The way in which this rule is implemented is absolutely critical to all ITI member companies and to U.S. national security and competitiveness more broadly. As such, we strongly encourage Commerce to continue to engage with stakeholders as it seeks to carry forth the IFR, including by issuing the voluntary licensing process for public comment. We look forward to working with Commerce as it seeks to implement the rule to ensure that any process results in a systematic, focused and calibrated approach that will effectively achieve the national security objectives laid out in the underlying EO. Please continue to consider ITI as a resource on this issue going forward, and do not hesitate to contact us with any questions regarding this submission.

Sincerely,

John S. Miller
Senior Vice President of Policy
and General Counsel

Courtney Lang
Director of Policy