US-China Business Council Comments on the Interim Final Rule for Securing the Information and Communications Technology and Services Supply Chain

Docket Number: DOC-2019-0005

March 22, 2021

On behalf of the 240 members of the US-China Business Council (USCBC, the Council) we appreciate the opportunity to submit comments to the Department of Commerce (Commerce) on the interim final rule (IFR) for Securing the Information and Communications Technology and Services (ICTS) Supply Chain. We recognize the national security concerns posed by malicious actors taking advantage of vulnerabilities in the US ICTS supply chain and support the US government's efforts to mitigate these risks. Furthermore, the Council acknowledges how the IFR makes limited progress on previously raised industry concerns about the November 2019 proposed rule.

Nonetheless, we believe that the scope of the IFR remains overly broad and will impose unnecessary costs on American businesses and cause undue economic harm to the United States. These concerns are corroborated by Commerce's own Regulatory Impact Analysis (RIA) which projects the IFR to directly impact 268,000 companies and affect over 4 million firms in total. The RIA projects annual compliance costs for companies to fall between the hundreds of millions and tens of billions of dollars. This extreme range of compliance costs is indicative of the overly broad powers of the IFR, which can cover virtually any ICTS transaction with even the most tenuous nexus to a "foreign adversary," including transactions that have already been completed. Companies both downstream and upstream of investigated entities will have to alter their practices to comply with prohibited or mitigated transactions. The rule's overly broad scope would make it difficult to provide the level of security intended since it would require vast amounts of resources for the government to implement and ultimately make it more difficult to identify the cases that truly pose a threat to security.

The RIA itself highlights how these costs will depend on factors beyond the control of companies, such as how often investigations are initiated, the priorities of the current Secretary of Commerce, and whether the investigations result in mitigation measures or the unwinding of transactions. These factors combine to make virtually every US company responsible for setting up costly compliance mechanisms for the IFR without knowing to what degree they will be subject to it.

The IFR also injects significant uncertainty into the business environment, hampering investment and, ultimately, American competitiveness. The uncertainty could discourage inbound investment into the United States as companies seek to insulate themselves from transactions that

could be subject to the IFR. It may also force US companies to move production from China, despite China being a critical source of revenue for them. This would dampen their competitiveness, and in turn, harm the United States' competitiveness and technological edge. Furthermore, the IFR will reinforce the growing reputation of American companies as unreliable suppliers.

Finally, exercising the IFR could prompt retaliation. If the United States moves forward with this rule, China will almost certainly draft measures providing similar authorities, compounding uncertainties for US companies in the global ICTS supply chain.

Limiting the trade of technology without clearly demarcating how companies can avoid infringing upon national security concerns will result in a less dynamic and less competitive US ICTS sector at a time when the United States and China are locked in intense competition to be the standard-bearer for advanced technologies.

The Council urges Commerce to revoke the IFR and draft new rules that address the relevant national security concerns through a process of robust industry consultation. Should revocation not be possible, USCBC hopes to work with Commerce to appropriately narrow the scope of transactions subject to the IFR and improve the regulatory processes involved. Designing high walls around small gardens will help ensure that the rule is implemented in an effective, predictable manner that mitigates the most critical security threats without undermining American competitiveness.

USCBC is encouraged to see the administration's February 24 Executive Order on America's Supply Chains (EO 14017), which provides a thoughtful, whole-of-government approach to supply chain security. We hope that revisions to the IFR will help bring it in line with this comprehensive approach that involves robust interagency coordination and broad consultations with industry.

Recommendations on scope:

- **Explicitly limit the IFR to domestic transactions:** At present, companies are confused as to whether there is an extraterritorial component to the IFR. It is particularly important to clarify that the IFR does not apply to wholly owned foreign subsidiaries of US companies. Including these companies under the purview of the IFR would impede the ability of US companies to operate globally, ultimately diminishing the dominance of US technology. Explicitly clarifying that the IFR is limited to inbound transactions would help companies accurately understand their compliance risks and requirements without undermining national security objectives.
- **Limit scope of nexus to foreign adversary:** Section 7.2 requires the review of transactions involving a "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary." While the IFR builds on the previously proposed rule to add more detail on this concept, it did not provide any meaningful clarification. For example, if a company employs a Chinese citizen in the United States, would that constitute a nexus to China? USCBC urges Commerce to specify a narrow definition of what sorts of relationships with a foreign adversary will trigger a review.

- **Further refine types of transactions covered:** The Council appreciates Commerce's efforts to define the types of ICTS transactions covered by outlining six types of transactions in Section 7.3 (a)(4) of the IFR. However, these updates did not meaningfully narrow the scope of the rule, as the six types of transactions listed cover nearly all types of ICTS transactions. This overly broad scope will make the IFR difficult and resource-intensive for the government to implement and will make it more challenging to identify true national security risks.
    - Commerce should explore widely accepted technical exceptions for transactions that cannot by their nature pose a security risk. For example, the US government currently relies on two exceptions to Section 889 of the *2019 National Defense Authorization Act* to mitigate risk in its own supply chains. Section 889 prohibits the US government from buying equipment produced by certain Chinese companies. One is for covered telecommunications equipment or services that "connect to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements." This is essential to ensure parties to transactions are not forced to disconnect machines from the internet for fear of violating the regulation. Another is for equipment or services that "cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles," since these products pose no risk.
    - The rule should clarify that use of information in the public domain and free updates and repairs are not covered under the scope of ICTS transactions subject to review.
    - For transactions that are not possible to completely exclude, Commerce should, at the very least, categorize them by risk and design different procedures based on level of risk. Commerce should work with industry to identify criteria and standards to mitigate security concerns in a more targeted manner. Companies can help identify processes and technologies that prevent foreign adversaries from obtaining sensitive data and infiltrating US critical infrastructure.
    - Commerce should eliminate or mitigate volume as an indicator of national security risk. The types of transactions covered under the IFR include ICTS products and services that have been sold to 1 million Americans within a 12-month period. However, it is not self-evident that volume by itself is a meaningful indicator of risk. There are likely low-risk, everyday technologies bought by millions of Americans that could be exempt. If it is not eliminated, volume should be paired with other risk-based factors to make clear to companies what specific transactions are being considered for review.
- **Limit retroactive applicability:** The IFR effectively grants Commerce the authority to prohibit an activity after it has occurred. Section 7.3 (a)(3) of the IFR allows the review of any ICTS transaction that is initiated, pending, or completed on or after January 19, 2021, but it also considers any follow-on services or updates to be transactions, meaning a large swath of transactions from before the IFR was implemented will ultimately fall under its authority given the complexity of ICTS supply chains.
    - Retroactive application of the IFR will have a disruptive effect on ongoing business relationships where contracts were established well before the IFR's existence. This gives companies the untenable responsibility of managing risks associated with unforeseen regulations. While they may be able to include

provisions in new contracts to address issues relating to the IFR, it will be difficult, if not impossible, to amend existing contracts. For companies with longstanding relationships or certain types of products only available from markets like China, it would be difficult to quickly and efficiently find alternative business partners.

    - As the IFR is written, any final determination could catch a product at any stage of its life cycle, impacting entities upstream and downstream in a complex global ICTS supply chain. For example, if a company stockpiles chips in the United States and it is later found that this is part of a prohibited transaction, is that company allowed to sell those chips even if it is years later? Even if a company is granted a license years ahead of when a particular piece of ICTS technology is meant to be incorporated into a consumer product, if a later administration moves the goal posts and finds it within scope, the company could face ruinous compliance costs. The IFR places the greatest risks and burden on the least knowledgeable party in the ICTS manufacturing and acquisition supply chain. Enacting a statute of limitations to outline a time limit for beginning a review after the initial transaction has been completed would help provide additional certainty to businesses. Specific time limits could differ based on the type of product and level of risk.

- **Limit liability to parties to the transaction:** The Council recommends that Commerce remove the "knew or should have known" standard in Section 7.2 borrowed from Export Administration Regulations and instead state affirmatively that only the parties to the transaction under review can be held liable for presenting a national security risk to the United States. A common carrier that is not part of the original transaction has no way of knowing whether any given product is or is not part of a prohibited transaction or a permitted transaction with mitigation measures in place.

Recommendations on process:

- **Institute a transparent, risk-based review approach:** While the IFR adds details on the types of information that will be considered, how it determines foreign adversary involvement, and factors for determining "undue or unacceptable risk," the updates provide little clarity on how the reviews will be conducted. USCBC urges Commerce to establish a rules-based review approach with transparent criteria. This approach should incorporate risk criticality categories (low, medium, high) or a risk scoring system and utilize different assessment methods and monitoring frequency based on risk.
- **Design risk-based licensing procedures:** USCBC is pleased to see that Commerce is working on a licensing regime for the IFR that would allow companies to have transactions pre-approved by Commerce, reducing uncertainty in the business environment. Licenses should provide companies safe harbor to ensure that Commerce will not later unwind their transactions after the fact. However, given the IFR's broad scope, it could still be burdensome to companies required to apply for large numbers of licenses, and it would take significant resources for Commerce to handle a large volume of license applications. In addition to a pre-clearance process, USCBC recommends that Commerce consider implementing a "trusted vendor" list that would provide a simplified application and approval process for lower-risk companies. Commerce could also

consider drafting a list of low-risk ICTS transactions and applying a simplified licensing process for these transactions.

- **Ensure no duplicative reviews:** USCBC is pleased to see that Section 7.3 (b)(2) of the IFR specifically exempts transactions that have undergone or are undergoing CFIUS review and also outlines an interagency consultation mechanism in Sections 7.104 and 7.108, but USCBC urges the government to go a step further. The rules should take into consideration all types of government reviews that also apply to transactions within its scope, like FCC licensing reviews, for example, to avoid duplication and mitigate the risk of contradictory rulings. Review under the ICTS rules should only take place where other legal authorities are deemed insufficient, so the rule should explicitly require a detailed assessment of why existing authorities are insufficient to mitigate the risk for each case.
- **Protect confidential business information:** Section 7.101 of the IFR allows Commerce to demand companies furnish confidential information under IEEPA authorities. Such authorities should be used sparingly and explicitly limited to cases where there is a clear national security rationale. While Section 7.102 outlines some measures to protect the confidentiality of information, the Council would like to emphasize how critical it is that Commerce protect confidential or proprietary business information to the fullest extent possible when issuing reports. This will help encourage parties to better cooperate with Commerce during the review process.
- **Provide transparency on information used for rulings:** Although the IFR provides additional detail on the process by which Commerce will analyze referrals, it does not provide a threshold on what type of information may be submitted and it does not establish a process by which a party subject to review would receive even a summary of the information that triggered the review. Without the ability for a company to respond to the information that a review is based on, it will be difficult for the government to assess the accuracy and completeness of the information it has received and clear up potential misconceptions. The Council recommends that Commerce adopt a process where companies are able to review and respond to information provided to Commerce that prompts the review of a transaction.
- **Ensure transparency of review notices and sufficient time to review initial determinations:** The IFR should explicitly clarify that parties to a transaction will be notified when a review is launched (rather than having to wait for the initial determination) to provide ample time to gather information that is important to the review process and provide input and evidence. For the same reasons, we also recommend extending the time for companies to reply to initial determinations to 45 days.
- **Include an appeal mechanism:** Section 7.105 of the IFR allows companies to respond to initial determinations within 30 days and provide evidence for why it may not apply or suggest remedial steps that would negate security concerns. This leaves the process entirely at the discretion of Commerce. The Council recommends instituting a formal interagency administrative appeals process to ensure transparent, rules-based due process for companies.
- **Allow a transition period for restrictions:** In cases where restrictions are imposed on ICTS transactions, it will be critical to allow for transition periods in order to avoid unintended disruptions to supply and employment and allow companies to fulfill contractual obligations.

- **Require an annual report to Congress:** To ensure transparency and accountability, the IFR should include a requirement for Commerce to provide an annual report to Congress detailing actions taken under its authority, similar to the annual reporting required for CFIUS.