APPENDIX: Discussion of Amendments to Interim Final Rule

ICTS Executive Order Regulatory Comments
Record of Implementation in Interim Final Rule

The following chart documents the degree to which the Department of Commerce (Department) addressed or incorporated the Chamber's comments in response to the Notice of Proposed Rulemaking Implementing the Executive Order Securing the Information and Communications Technology and Services Supply Chain (NPRM).

The Interim Final Rule (IFR) responds to a number of the Chamber's suggestions. However, the overall effect of these changes is modest. The IFR continues to lack the procedural and substantive safeguards featured in similar statutory and regulatory regimes, such as CFIUS, and its potential application across various industries, technologies, and services remains quite broad. Moreover, despite the introduction of certain limitations, the Secretary reserves considerable discretion to select targets for review and to consider mitigation measures.

One key outstanding question relates to the proposal from the business community to establish a formal or informal pre-clearance process where parties can submit transactions for pre-clearance review. The IFR states that within 60 days of publication Commerce will publish procedures "to allow a party or parties to a proposed, pending, or ongoing ICTS Transaction to seek a license." The procedures "will establish criteria by which persons may seek a license to enter into a proposed or pending ICTS Transaction or engage in an ongoing ICTS Transaction." These procedures establishing the licensing process will go into effect within 120 days of publication—that is, May 19, 2021. A robust and accessible license program could alleviate some of the commercial uncertainty caused by the Executive Order and its implementing regulations, but there is not enough detail provided in the IFR to determine the level of relief that may be provided by the forthcoming license program.

The chart below is divided into sections based on key categories of comments regarding the Proposed Order and provides our response to the IFR.

* * *

1. Ensure Accountability and Interagency Collaboration Through Procedural Guardrails

Chamber Comment on NPRM	*Adopted?*	*Chamber Response*
If the Department publishes a public report, the data should be high level categories of the number of transactions reviewed, blocked, and mitigated, category of ICTS involved; and national security rationale.	Partial	The Chamber supports the decision in the IFR to not mandate publication of an annual report with general statistics and information on ICTS transactions reviewed by the Department.
Establish more formalized interagency review process, including by further defining the interagency role and creating a mechanism for formal convening of agency heads or voting on whether transactions are subject to the Rule.	Partial	The IFR sets forth two stages of interagency consultation. The first requires the Secretary to "notify the appropriate agency heads, and, in consultation with them, shall determine whether the ICTS Transaction meets the criteria set forth in § 7.103(c) (regarding undue and unacceptable risk)" when the Secretary determines that an ICTS transaction likely poses an undue or unacceptable risk. (*See* IFR § 7.104 (p. 67)) The second is after the Secretary receives and considers the effects of a submission from a party to an ICTS Transaction subject to an initial determination. At that point, the Secretary "shall consult and seek the consensus of all appropriate agency heads prior to issuing a final determination." § 7.108(a)-(b) (p. 69). However, the Chamber urges the Department to further define the term "consultation" to ensure it is more than a mere notification. Further, the Department should also adopt a process whereby agency heads would be required to convene for a session or to conduct a vote to ensure consensus on whether a transaction is subject to the Rule prior to elevating any disagreement to the President.

2. Provide Clarity and Calibrate the Scope of the Elements of the Order and Rule

Comment on NRPM	*Adopted?*	*Chamber Response*
Define "dealing in" based on definitions contained in Securities Act of 1934, as "engaging directly in a financial transaction for the offering, buying, selling, or trading of prohibited ICTS."	Partial	The IFR defines an ICTS transaction to mean "any acquisition, importation, transfer, installation, dealing in, or ***use of*** any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download." IFR § 7.2 The IFR additionally provides that an ICTS transaction may also include "any other transaction, the structure of which is designed or intended to evade or circumvent the application of the Executive Order." There is a risk of creating a misleading perception that information in the public domain that is published and that is generally accessible or available to the public without exchange of payment is intentionally designed to evade the rule or subject to review under the rule. Adoption of such a broad definition without further clarification of the types of transactions that are included will create uncertainty about the overall scope of coverage of the IFR within industry. Along these lines, it is not clear if ICTS transaction include the 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 for charitable or donative purposes) may 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. The Chamber therefore recommends that the Department clarify the ICTS transactions definition to explicitly exclude information in the public domain as well as no cost updates and repairs.

Comment on NRPM	*Adopted?*	*Chamber Response*
The Department should provide a clear safe harbor for companies that are not directly involved in transactions involving a foreign adversary.	Partial	The Chamber appreciates the Department's efforts to provide a carve out for common carriers in the Section 7.2 definition of "party or parties to a transaction." However, by including an exception "to the extent that a common carrier knew or should have known (as the term "knowledge" is defined in 15 CFR 772.1[1]) that it was providing transportation services of ICTS …that has been prohibited…," the Department effectively negates effect of the common carrier carve out. Although Section 7.109 of the regulations states that the Secretary will issue a final determination as to whether the ICTS Transaction is "prohibited, not prohibited or permitted pursuant to mitigation measures which shall be published in the Federal Register," a common carrier would still not be able to know whether a particular shipment was related to the specific ICTS Transaction given the limited information the Department plans to disclose in the Federal Register notice. Without adequate notice, a common carrier has no reasonable means of making a good faith effort to comply, and as such, could never be deemed to have "knowledge" of such a prohibited transaction. The Department should modify the IFR to carve out an express safe harbor provision for transportation companies along the supply chain, such as common carriers, freight forwarders, and brokers, who are not parties to the ICTS transaction. Specifically, Section 7.2 should expressly state that common carriers do not fall within the scope of the regulations without including the 15 CFR Section 772.1 knowledge exception. Alternatively, if the Department decides to include common carriers within the scope of this regulation, the rule should expressly state that a common carrier can be held liable only if it has actual knowledge that it is carrying an item that violates a specific restriction by the Commerce Department without reference to the definition of "knowledge" in the EAR at 15 CFR 772.1.

[1] *Knowledge*. Knowledge of a circumstance (the term may be a variant, such as "know," "reason to know," or "reason to believe") includes not only positive knowledge that the circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence. Such awareness is inferred from evidence of the conscious disregard of facts known to a person and is also inferred from a person's willful avoidance of facts. 15 C.F.R. 772.1.

Comment on NRPM	***Adopted?***	***Chamber Response***
Whether Foreign Subsidiaries That Are Wholly Owned by U.S. Entities Are Captured Under the IFR	Partial	Commerce should clarify that the scope of the IFR's application to non-U.S. persons, does not apply to foreign subsidiaries that are wholly owned by U.S. entities. The IFR states that it applies only to ICTS transactions that are "conducted by any person subject to the jurisdiction of the United States" or "property subject to the jurisdiction of the United States." IFR § 7.3(a-b). The ICTS EO defines "United States person" as "any United States citizen; any permanent resident alien; or any entity organized under the laws of the United States or any jurisdiction within the United States (including such entity's foreign branches)." ICTS Executive Order §3(e). Were Commerce to define its jurisdiction to broadly include foreign subsidiary entities organized under other jurisdictions, it would impinge the ability of a foreign company to conduct transactions outside of the United States and on the ability of U.S. companies to operate in the global marketplace. This would diminish U.S. technology dominance and influence. Commerce should amend Section 7.3 to clarify that the Rule applies only to transactions in which the ICTS in question enters the United States or is provided and used in the United States by U.S. persons. Such a clarification would be consistent with the nature of the national emergency declared in the ICTS Executive Order. The Order states that to deal with the threat of ICTS emanating from foreign adversaries, "additional steps are required to protect the security, integrity, and reliability of information and communications technology and services ***provided and used in the United States***" (emphasis added). This clarification would limit potentially adverse economic consequences of the Rule—such as limiting global business opportunities, potentially prompting retaliation by foreign countries—without sacrificing its ability to protect U.S. national security.
Ongoing Transactions	No	Section 7.3(a)(3) of the IFR states that the regulations will apply to ICTS transactions that among other things are "initiated, pending, or completed on or after January 19, 2021, ***regardless of when any contract applicable to the transaction is entered into, dated, or signed or when any license, permit, or authorization applicable to such transaction was granted.***" (Emphasis added.) The retroactive application of the IFR to existing contracts will have a disruptive effect on ongoing business relationships since those contracts would have been established well before the existence of the IFR or of Executive Order 13873. Parties to existing contracts have not had the ability to consider these new requirements in diligence or planning for such transactions. Thus, these parties may not have built in provisions to their contracts to address significant issues relating to these regulations, such as the responsibility for applying for and seeking a license, or termination of the relationship in the event of an adverse decision by Commerce. Such parties may also have a long-established relationship and may not have the ability to switch to an alternative business partner quickly or efficiently. Moreover, the retroactive application of the IFR to existing contracts not only puts companies in an untenable position of trying to manage risks associated with unforeseen regulations; it also expands the scope of transactions that are subject to Commerce's review to a nearly impossible number for Commerce to effectively manage. Additionally,

Comment on NRPM	*Adopted?*	*Chamber Response*
		an ongoing transaction, if reviewed, should only be reviewed upon a showing of an actual, identifiable, unmitigated, and active security breach or discrepancy. For each of these reasons, we strongly encourage Commerce to exclude transactions arising from existing contracts from the scope of the IFR and to instead focus on new contracts entered into after the effective date of the IFR.

3. Establish Procedures for Government Review, Including Sufficient Notice, Pre-Clearance Discussions, and Post-Review Certainty

Comment on NRPM	*Adopted?*	*Chamber Response*
Extend timeline for parties to respond to preliminary determination beyond 30 days (suggested minimum of 60 days).	No	The Chamber continues to recommend a minimum of 60 days to respond to a preliminary determination. While the scope of an investigation may vary, it is unreasonable to expect companies large and small to respond to a preliminary determination within 30 days. Additional time will allow a firm time to respond substantively.
Establish formal or informal pre-clearance process by which parties can submit transactions for pre-clearance review.	TBD	The Chamber looks forward to reviewing Commerce's proposed procedures to allow a party or parties to a proposed, pending, or ongoing ICTS Transaction to seek a license.
Require standard or threshold for what type of information may be submitted for review by outside private parties.	No	The IFR maintains the provision permitting private parties to submit information via a secure portal for review by the Department. We strongly urge the Department to eliminate this provision or to provide additional due process protections, such as confidential treatment and procedures to protect against the inadvertent disclosure of the information submitted to the parties tothe transaction under review and a requirement that submitters provide a sworn affirmation under penalty of perjury that all of the provided information is true and correct to the best of their information and belief, and that the submitter believes in good faith that a transaction warrants investigation under the standards of the Department's rules. Although the IFR expands on the process by which the Secretary will analyze private-party referrals—nominally requiring the Secretary to weigh the referral against the procedures established in the Rule—in practice, the IFR grants the Secretary broad discretion in determining whether to act on such referrals and does not provide a threshold on what type of information may be submitted or any protection against misuse of the submission process by competitors. *See* IFR § 7.103(b).
Provide an entity subject to review the information submitted by a private outside party, should that outside party's information trigger review.	No	The IFR does not establish a process by which a party subject to review would receive at the very least a summary of the information provided by a private party if that information triggered review. Although companies may be subject to obligations to submit accurate information to the Government under existing statutes such as the False Statements Act[2], without the ability for a company to respond to information that has been submitted by a third party, it may be difficult for the U.S. Government to assess the accuracy and completeness of the information it has received or to understand if that information is false or misleading. We request that Commerce adopt a process whereby entities are able to review and respond to any information provided to Commerce that prompts the review of a transaction.

[2] *See* 18 U.S.C. § 1001(a) ("Except as otherwise provided in this section, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully—(1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact; (2) makes any materially false, fictitious, or fraudulent statement or representation; or (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry; shall be fined….").

4. Address Interplay of Overlapping Regulations

Comment on NPRM	*Adopted?*	*Chamber Response*
Establish that authorities implemented by Rule should only be used where other legal authorities are not sufficient to address identified national security risk, such as by applying positive presumptions to transactions that have already undergone overlapping or similar review under existing regulatory processes. The strongest measure would clarify that "peer-reviewed" transactions are not subject to subsequent review, absent unusual or compelling circumstances.	Partial	The Chamber urges the Department to better calibrate this IFR with existing federal authorities. The IFR establishes that nothing in the Rule "shall be construed as altering or affecting any other authority, process, regulation, investigation, enforcement measure, or review provided by or established under any other provision of Federal law, including prohibitions under the National Defense Authorization Act of 2019, the Federal Acquisition Regulations, or IEEPA, or any other authority of the President or the Congress under the Constitution." § 7.5 (pp. 59-60). The IFR further provides that the Rule does not apply to ICTS Transactions that CFIUS is "actively reviewing, or has reviewed, as a covered transaction." § 7.3(b)(2) (p. 58). Further, the IFR should incorporate language similar to that contained in the CFIUS statute, establishing that CFIUS may seek to mitigate a risk "not adequately addressed by other provisions of law." 50 U.S.C. § 4565(d)(4)(B). Moreover, although the IFR states that the Rule does not apply to ICTS Transactions that CFIUS has reviewed, it does not appear to extend that safe harbor to reviews conducted under other statutory or regulatory processes, including Section 889, Team Telecom, the FCC restrictions on use of certain telecommunication equipment in U.S. 5G networks, transactions subject to the Export Administration Regulations, or Office of Foreign Assets Control regulations. This review process should not duplicate efforts of other agencies and should only apply when the transaction is not subject to the regulations listed above. Thus, we would encourage Commerce to extend the safe harbor to these processes as well.

5. Ensure Confidentiality in Review Process

Comment on NPRM	*Adopted?*	*Chamber Response*
Describe procedures to protect business confidential information submitted for review, including by requesting that Congress provide statutory protection.	Partial	The Chamber urges the Department to provide additional protections to provide businesses with the opportunity to object and/or redact any business confidential information prior to disclosure in any circumstance.

6. Define Robust Procedures for Waivers, Appeals, Due Process, and Mitigation

Comment on NPRM	*Adopted?*	*Chamber Response*
Incorporate the exceptions featured in Section 889 of the FY2019 National Defense Authorization Act that would identify classes of transaction excluded from prohibition: (1) a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; (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.	Partial	The IFR does not contain any notable exceptions for those transactions that cannot by their nature pose any risk to the United States and its people. Instead, the IFR requires parties in virtually all cases to either (i) prepare, submit, and wait for a decision on a license, or (ii) to enter into or continue business relationships under a state of persistent uncertainty as to whether Commerce may ultimately require the parties to terminate the relationship or force implementation of mitigating measures. Outlining universally recognized technical exceptions to the IFR would increase certainty within industry and would allow Commerce to focus its reviews on those transactions that have the greatest relative ability to pose risk. The use of technical exceptions is not new to ICTS-focused regulations. The U.S. Government currently relies on two principal exceptions to the Section 889 prohibitions that mitigate foreign risk in the Government's own supply chains. Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 prohibits the U.S. Government from buying (as of August 2019)—or contracting with an entity that uses (as of August 2020)—equipment, systems, or services that use covered telecommunications equipment or services as a substantial or essential component of any of system produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities) or, in certain cases, telecommunications or video surveillance equipment or services produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of those entities) (collectively, "Covered Telecommunications Equipment or Services"). The IFR recognizes two technical exceptions that are now known and familiar to Government contractors and commercial organizations that sell products or services to Government contractors. The first exception applies to Covered Telecommunications Equipment or Services that "connect to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements." This first exception ensures that parties to transactions are not forced to disconnect machines from the internet or from telecommunications services for fear of violating the regulation. The second exception applies to Covered Telecommunications 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." This second exception exempts those products or services that do not have the capability of posing any risk to the Government. Adopting these exceptions under the IFR would increase certainty regarding its intended scope. Indeed, these two exceptions were recently adopted in Section 841 of the William M. (Mac) Thornberry National Defense

Comment on NPRM	*Adopted?*	*Chamber Response*
		Authorization Act for Fiscal Year 2021, which relates to the supply chain risks associated with printed circuit boards. Accordingly, we recommend that Commerce consider adopting the two recognized technical exceptions discussed above and also to engage in further dialog with industry about other potential technical exceptions that could be implemented for the mutual benefit of industry and Commerce.
Adopt standard of "reasonable care" where companies that follow best practices for due diligence and care in evaluation of goods and services should be given some level of deference for good faith.	No	The IFR provides no actionable information to businesses to create a compliance program. The Chamber urges the Department to adopt a standard of reasonable care and to provide voluntary "best practices" to assist in reducing national security concerns in ICTS transactions.
Due Process	Partial	In relying on the authorities granted under the International Emergency Economic Powers Act (IEEPA) without any additional statutory authorization, the ICTS Executive Order deprives businesses of proper due process. Moreover, despite the changes made to the Rule in the IFR, the Rule continues to grant the Secretary of Commerce an expansive scope of authority to disrupt the commercial operations of private companies and deprive those companies of property without providing sufficient due process. Due process is important for companies to be able to anticipate compliance and build it into the fabric of their businesses. Further, the lack of disclosure of the information which "accuses" parties of engaging in a risky transaction, deprives companies of the ability to effectively defend and protect against such accusations in a proactive manner. A more precise rule that provides companies with clear understanding of the concerns and expectations for compliance would give U.S. companies the opportunity to in mitigate the concerns early and consistently.