Comments on the Commerce Department's
Securing the Information and Communications Technology and Services ("ICTS")
Supply Chain Interim Final Rule ("Rule")
Docket No. 210113–0009
March 22, 2021

The Coalition of Services Industries (CSI), based in Washington, D.C., has represented the interests of the services sector since 1982, shaping policies to facilitate the growth of services trade and promoting greater awareness of the role of services in the U.S. economy. Our members include companies that provide services both domestically and internationally, including information and communication technology services, financial services, express delivery and logistics, media and entertainment, distribution, retail and professional services.

Thank you for the opportunity to comment on the Interim Final Rule implementing the executive order on "Securing the Information and Communications Technology and Services Supply Chain." We have briefly outlined our objections to elements of the Rule at the beginning of our comments, after which we describe our concerns in greater detail further below.

***

While we appreciate that the Commerce Department has made certain changes to the initial draft Rule, the breadth of the Rule, coupled with the Department's broad discretion to review transactions, creates significant new business risks and may ultimately chill investment and transactions that would benefit U.S. businesses and consumers. Similarly, its application to pending or completed transactions into the future will create considerable uncertainty for companies and potentially make U.S. companies less competitive.

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 that "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 mitigate the concerns early and consistently.

Government interventions in commercial activity should follow a transparent process, be clearly defined in scope, and be narrowly tailored to specific security risks. However, as written, the Rule is overly broad and seems poised to exact very high compliance costs. According to a cost analysis by Commerce

released on February 18, the Rule could impact potentially millions of firms at compliance costs estimated between $1B and $52B—and annualized costs of $235M-$20B.

From the standpoint of industry, supply chain security is already a business imperative. Most U.S. companies are willing and committed to mitigating security risks and can be valuable partners in helping Commerce develop real criteria and standards for mitigating the concerns identified in a more targeted fashion. Companies can identify processes and technologies to help prevent foreign adversaries from obtaining sensitive data and infiltrating U.S. infrastructures. To consider one example, the communications sector is engaged in several initiatives underway, including the DHS ICT Supply Chain Task Force, and the sector has independently prioritized supply chain security efforts.

In short, we believe it is possible to enhance national security without needlessly hindering U.S. trade and investment. Failure to maintain this balance might result in the U.S. losing its competitive edge in many emerging areas. This could diminish our innovative base, ultimately negatively impacting the economy as well as our ability to develop intelligence and military systems to counter those same adversaries.

To the extent the Department maintains its current approach and intends to finalize the Rule, we have proposed further changes in more detail below:

Definitions: To add greater clarity for companies and to be consistent with existing regulations, Commerce should amend existing definitions or add new definitions.

"Person Owned by, Controlled by, or Subject to the Jurisdiction or Direction of a Foreign Adversary." We urge Commerce to narrow this definition, which would currently include "any corporation, partnership, association, or other organization organized under the laws of a nation-state controlled by a foreign adversary." This is extremely broad and runs the risk of including U.S. companies' non-U.S. subsidiaries in China even though such entities generally present a lower national security risk. We urge Commerce to strike the aforementioned language from the definition and explicitly acknowledge that corporations, partnerships, associations, or other organizations, wherever organized or doing business, that are not controlled, or owned by a foreign adversary do not warrant particular scrutiny.

"Any Person Subject to the Jurisdiction of the United States." We urge Commerce to define this term to clarify that it has the same definition as "United States person," as an ICTS transaction conducted by a subsidiary owned or controlled by a U.S. person generally presents lower national security risks due to oversight by U.S. persons. Currently the Rule 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)." It is unclear if "any person subject to the jurisdiction of the United States" is intended to: (1) have the same definition as "United States person"; or (2) broadly cover non-U.S. subsidiaries of U.S. persons, as the term is used in the Cuban Asset Control Regulations.[1] Leaving the term undefined brings uncertainty to U.S. companies with regard to their non-U.S. subsidiaries.

Additional Definitions. While we appreciate Commerce's attempt to better describe certain terms in response to industry's comments, many are still vague and unclear to industry. Better defining terms such as "undue or unacceptable risks," and "integral" will help companies to identify ICTS Transactions of concern.

"Party or Parties to a Transaction." The IFR should be revised to clarify that only the parties to the ICTS Transaction itself can be held liable for violations of the regulation.

In addition, we urge Commerce to add language excluding telecom carriers for general transmissions of data. Currently various sanctions programs include carveouts for common carriers and telecoms. Additionally, the Export Administration Regulations ("EAR") exclude from the definition of "export" the sending, taking, or storing of technology or software that is, among other things, secured using end-to-end encryption because the telecoms cannot see the technology or software transmitted over their networks. We recommend a similar exclusion be added here:

> "For purposes of this rule, this definition does not include telecommunications carriers in a transaction where a telecommunications carrier is transmitting data on behalf of the general public, except to the extent a telecommunications carrier knew or should have known (as the term "knowledge" is defined in 15 C.F.R. § 772.1) that it was providing transmission services of ICTS to one or more of the parties to a transaction that has been prohibited in a final written determination made by the Secretary or, if permitted subject to mitigation measures, in violation of such mitigation measures."

Common carriers that transport goods that may be part of, or related to, an ICTS Transaction should be excluded from the definition of a "party or parties to a transaction" and not be held liable for civil or criminal violations of the regulations.

CSI 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.

CSI encourages the Department to 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

---

[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.

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.

Scope of Transactions: Commerce should clarify the scope of ICTS Transactions, including the following:

Retroactive Application. 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 of May 15, 2019 (the "ICTS Executive Order").

The Rule also defines "ICTS Transactions" to include "ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download." This broad definition includes the execution of any provision of a managed services agreement (MSA), even if the contract was entered into or the activity began before January 19, 2021. Large corporations typically enter into multi-year managed services agreements with repeat customers and issue related purchase orders. The Rule as drafted would cover purchase orders initiated, pending, or completed on or after January 19, 2021, but it does not explicitly state that the underlying MSAs entered into, signed, or dated, or POs completed, before January 19, 2021 are *not* ICTS Transactions. As a result, the government's approach stands to raise doubts about the validity of a wide swath of transactions, as we understand the intent of the Rule.

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, 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.

Clarify that Foreign Subsidiaries That Are Wholly Owned by U.S. Entities Are Not Captured Under the IFR. It is also important for Commerce to 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 Executive Order 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.

"Use of" Should Be Applied to Exclude Information in the Public Domain and Should Not Cover No-cost Updates or Repairs Important for Security. The Interim Final Rule ("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 (emphasis added.) 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." As written, the rule could create the 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. Adoption of such a broad definition without further clarification of the types of transactions that are included creates uncertainty about the overall scope of coverage of the IFR within industry.

Along these lines, 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. Also, 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 a 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 the Department of Commerce ("Commerce") clarify the ICTS transactions definition to explicitly exclude information in the public domain as well as no cost updates and repairs.

Revise Process for Determining Foreign Adversary Involvement. We urge Commerce to revise the newly added process that could pull in parties for having "ties" to a foreign adversary. Amendments to the process for determining whether a party is a foreign adversary, include personal and professional ties between the party, its officers, officials, employees, consultants, or contractors and a foreign adversary.[4] This factor is vague, overbroad, and could lead to absurd results as the term "tie" is not

defined. For example, a person could have a personal tie to a foreign adversary for simply meeting a Chinese national once. We urge Commerce to narrow the scope of potentially covered parties by either defining "tie" or by narrowing the language along the following lines: "whether the person—including its officers, directors, or similar officials employees, consultants, or contractors—is a business partner or close associate or family member of a foreign adversary."

Clarify Scope of "Software, Hardware, or Any Other Product or Service Integral to Data Hosting or Computing Services." One of the six main types of ICTS includes "[s]oftware, hardware, or any other product or service integral to data hosting or computing services, to include software-defined services such as virtual private servers, that . . . is expected to use, process, or retain, sensitive personal data on greater than one million U.S. persons at any point over the twelve (12) months preceding an ICTS Transaction."[5] This language is based on the definition of "sensitive personal data" in the CFIUS regulations, but its meaning is unclear in the Rule. Commerce should more closely follow the CFIUS language and revise § 7.3(a)(4)(iii) to clarify the person – not the software – is expected to use the software to use, process, or retain personal data:

> "Software, hardware, or any other product or service integral to data hosting or computing services, to include software-defined services such as virtual private servers, that uses, processes, or retains, or ~~is expected to~~ software-defined services for which the person subject to the jurisdiction of the United States has demonstrated a business objective to use, process, or retain, sensitive personal data on greater than one million U.S. persons at any point over the twelve (12) months preceding an ICTS Transaction."

Clarify Hardware Devices (e.g., Handsets) that Do Not Warrant Particular Scrutiny. While Commerce did not adopt an earlier suggestion to create risk categories, we acknowledge the new language indicating that transactions solely involving personal ICTS hardware devices, such as handsets, do not warrant particular scrutiny. However, Commerce did not define the scope of personal ICTS hardware. We urge Commerce to adopt the August 2019 Huawei Temporary General License's approach of replacing the undefined term "handsets" (in the May 2019 Temporary General License) with a defined term for "personal consumer electronic devices": "phones and other personally-owned equipment, such as tablets, smart watches, and mobile hotspots such as MiFi devices."[3]

Apply Technical Exceptions, Including Those Set Forth under the "Section 889" Supply Chain Regulation. As written, 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.

Along these lines, the use of technical exceptions is not new to ICTS-focused regulations. Indeed, 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 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 dialogue with industry about other potential technical exceptions that could be implemented for the mutual benefit of industry and Commerce.

Revise Second Interagency Consultation Process (Section 7.108). The preamble explains that, at this stage of the review, Commerce will consider other agencies' views, which may be informed by "relevant public-private working groups and advisory committees with which they convene or engage. For instance, DHS's views could incorporate input from the Supply Chain Risk Management Task Force . . . or other advisory committees that provide regular opportunities for industry and the regulated community to provide feedback.[6] Commenters expressed concerns that similar language in the Proposed Rule's referral process (e.g., Commerce consulting the public via public-private working groups or advisory committees) could lead to anti-competitive behavior.

This concern remains in the Second Interagency Consultation Process; e.g., a company that is a prominent member of a public-private working group could be motivated by business reasons to recommend prohibiting a competitor's ICTS Transaction to the relevant agency, which could lead to Commerce espousing that view. Commerce should strike this language from the preamble, as it is not in § 7.108.

Process Refinements: Various parts of the review process lack clarity and therefore cause uncertainty for business. We urge Commerce to continue to refine various procedural parts of the review process.

Confidentiality and Federal Register Publications. We urge Commerce to strike provisions authorizing publication of initial and final determinations in the Federal Register because: (1) the determinations themselves should be treated as confidential business information; and (2) publishing determinations could detrimentally impact businesses financially, lead to competitive disadvantages, and cause

reputational harm. At minimum, parties should be able to consent in writing prior to Federal Register publication.

Additional Time to Respond to Initial Determinations. Given the complexity of the Rule and cross-border nature of ICTS Transactions, Commerce should extend the response period to either 30 business days or 45 days. Under the Rule currently, parties must respond to Commerce's notification of an initial determination within 30 days of service (e.g., to assert that circumstances prompting the initial determination no longer apply). The government often gives parties more time to respond to novel trade actions, which can be helpful for all parties, including allowing the U.S. government to more fully understand the response process and implications of the action.

Sunset Provision for Mitigation Measures. For ICTS Transactions permitted after the adoption of mitigation measures, we urge a regular review of the mitigation measures. Section 7.109 could include a sunset provision requiring Commerce to review mitigation measures every five years to determine whether the measures must remain in force or can be revised or terminated by mutual agreement of the parties.

Exclusions. Commerce should consider exclusions from the Rule for "the export, reexport, or transfer of ICTS items that are subject to the EAR and that are authorized for export, reexport, or transfer pursuant to any export license issued by the U.S. Department of Commerce, Bureau of Industry and Security." Further, since the Rule carves out ICTS acquisitions by U.S. persons subject to DCSA FOCI mitigation, Commerce also should add an exclusion for: "the acquisition, importation, transfer, installation, dealing in, or use of ICTS items by a United States person as a party to a transaction that is subject to a CFIUS mitigation agreement." At minimum, Commerce should exclude the "acquisition" of ICTS items by U.S. persons subject to CFIUS mitigation agreements.

Mitigation Consistency. Concerns remain that Commerce's ICTS mitigation measures may conflict with other mitigation measures implemented as part of other US government transaction reviews (e.g. CFIUS). Absent excluding certain transactions from review, Commerce should ensure proper consultation with other agencies that have already implemented mitigation as part of a transaction approval to help avoid conflict between regimes.

Licensing Regime: We urge Commerce to work with industry in developing the licensing regime, and that such regime is implemented so as not to hamper legitimate business activities.

ICTS License Application Format. Given the broad scope of the interim final rule, a high volume of transactions will likely be impacted by the rule, which in turn will likely result in numerous licensing requests. Licensing procedures that are familiar to both Commerce and the industry will help facilitate the review process for Commerce and reduce the amount of uncertainty for the industry surrounding the licensing process.

For example, Export Administration Regulations ("EAR"), export license applications with Commerce are filed with what is called Form BIS-748P. For certain export transactions, a letter of explanation includes additional information about the transaction. Commerce's export licensing procedures with the Form BIS-748P are much more streamlined than the CFIUS review process and the letter of explanation can often help applicants provide more context to a transaction. The letter of explanation can include the following information: (1) an explanation of why the transaction is a covered ICTS transaction; (2) the identities of all parties to the ICTS transaction; (3) a description of the type of ICTS involved, including

technical information and exhibits; (4) the location(s) where the ICTS will be used; and (5) the end uses of the ICTS.

Supplemental Information Requests and Timing for Responses. Similar to CFIUS and export license reviews under the EAR, during the course of an ICTS license application review Commerce will likely request follow-up information from applicants. The applicants should be allowed at least two business days to respond to requests and reasonable requests for extensions should be liberally granted.

ICTS License Review Policy. In the preamble to the interim final rule, Commerce acknowledged that "ICTS Transactions solely involving personal ICTS hardware devices, such as handsets, do not warrant particular scrutiny." When applicable, Commerce should provide a license review policy for certain types of transactions to inform the public on the level of national security for certain ICTS transactions (e.g., case by case review, presumption of denial).

ICTS License Review Timeline. The preamble to the interim rule indicated that the license application reviews will be conducted on a fixed timeline not to exceed 120 days and that if Commerce does not issue a license decision 120 days from accepting a license application, the application will be deemed granted. The 120-day timeline (i.e., 4 months) is too long and will significantly impact business operations for companies operating in ICTS industries. Compare this timeframe with other review timeframes currently in existence:

- CFIUS Review Timelines: CFIUS has a 30-day assessment period for declarations and for notices it has an initial 45-day review period that can then be extended to a 45-day investigation period.
- EAR License Review Timelines: Commerce has 90 calendar days to resolve a license application or refer it to the President.
- ITAR License Review Timelines: The Department of State is provided 60 days to adjudicate ITAR-related license applications with national security exceptions.

Commerce should consider a staged review timeframe. For example, it could provide for an initial 30-day review period for ICTS license applications. After the 30-day period, Commerce can: (1) approve the license application; (2) initiate another 30-day review period; or (3) not take action and the license would be deemed granted after the 30-day period.

ICTS Licensing Determination. Under the EAR and ITAR, license applications are granted for a certain amount of time (e.g., generally up to four years under the EAR). On the other hand, when parties to a transaction file with CFIUS and CFIUS completes its review, the parties avail themselves of a safe harbor, which prevents any further action by CFIUS after it has reviewed the transaction. As the ICTS interim final rule already excludes ICTS transactions being reviewed or previously reviewed by CFIUS, where Commerce decides not to prohibit or impose mitigation on an ICTS transaction, Commerce should provide the parties a safe harbor that prevents any further action from Commerce after it has reviewed an ICTS transaction.

Other concerns.

Private Party Submissions. The IFR maintains the provision permitting private parties to submit information via a secure portal for review by Commerce. We strongly urge Commerce to eliminate this provision or to provide additional due process protections, such as disclosure of the information submitted to the parties to the transaction under review.

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. *See* IFR § 7.103(b). Moreover, 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 with a response from the company whose transaction or product is at issue. 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.

Enforcement guidelines. We urge the Department to promulgate enforcement guidelines. Section 7.200 of the interim final rule sets forth civil and criminal penalties for violations of final determination or directions issued by the Department. The interim final rule does not include enforcement guidelines, which are particularly important given that prohibitions may apply to any ICTS Transaction "that is initiated, pending, or completed on or after" January 19, 2021.

The Department should issue enforcement guidelines, including the opportunity to voluntarily disclose potential violations and mitigation for such disclosures. The Office of Foreign Assets Control's Enforcement Guidelines, found at 31 CFR Part 501, Appendix A, can be used as a model. Enforcement guidelines that include mitigation for voluntary disclosures can encourage industry to come forward to the agency, assisting the agency with enforcement.

[1] See 31 C.F.R. § 515.329(d).
[2] Id. at 4924.
[3] 84 Fed. Reg. 43,487, 43,488 (Aug. 21, 2019).
[4] Id. at 4926.
[5] 86 Fed. Reg. 4909, 4924 (Jan. 19, 2021) (emphasis added).
[6] Id. at 4918 (emphasis added).

[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….").