ITI Promoting Innovation Worldwide

April 28, 2021

Ms. Wynn Coggins
Acting Deputy Secretary
U.S. Department of Commerce
1401 Constitution Ave NW
Washington, DC 20230

RE: ITI Comments Responding to Commerce Department ANPRM on Securing the Information and Communications Technology and Services Supply Chain Licensing Process (RIN 0605-AA60: ANPRM; DOC-2021-0004)

Dear Acting Deputy Secretary Coggins,

The Information Technology Industry Council (ITI) appreciates the opportunity to continue its engagement with the Department of Commerce ("Commerce") as it develops the pre-clearance and/or licensing process associated with the Interim Final Rule, which implements Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain*.

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 addressing risks to global information and communications technology (ICT) supply chains. We believe it is imperative that government and industry work together to achieve the trusted, secure, and reliable global ICT supply chain that is essential for protecting national security and an indispensable foundation for supporting innovation and economic growth.

In the comments we submitted in response to the Interim Final Rule, we recommended that Commerce put forth the licensing process for public comment. We appreciate that Commerce has done so. However, given the underlying breadth of the Executive Order and associated rule on which the license process seeks to build, there is a resultant lack of clarity regarding which entities, products, services and transactions are in fact in scope for potential review by Commerce, making it challenging to provide meaningful responses to the questions outlined in the ANPRM. Indeed, the

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

broad and vague scope with respect to which ICTS Transactions are covered in the IFR not only makes it difficult to effectively implement the rule, but also will have a major impact on the effectiveness and ultimate viability of any voluntary pre-clearance/licensing process, which will ultimately hinge on the ability to provide effective notice to companies seeking to pre-clear transactions. A clear and narrowed scope on the front end is absolutely imperative to provide parties with the guidance and notice they need to effectively use any pre-clearance/licensing regime.

Below, we share some high-level thoughts regarding the proposed pre-clearance/licensing process, including recommendations on important aspects that should be included in the process. Following this, we provide responses to the specific questions that are posed in the ANPRM.

Implementation of the rule should be delayed until there is a viable voluntary pre-clearance/licensing process in place. We encourage Commerce to seriously consider delaying implementation of the rule until a viable voluntary pre-clearance/licensing process has been established. At present, the IFR provides the Secretary broad authority to review practically every single ICTS Transaction with any nexus to an identified "foreign adversary," and casts a cloud of uncertainty over all other ICTS transactions given the list of named foreign adversaries could change at any time. When combined with the Secretary's additional power to block and unwind deals and the absence of any effective voluntary pre-clearance/licensing process, the fact that the rule is "live" creates immense uncertainty in the business community that will result in an unnecessary, chilling effect on innovation and commerce. As Commerce is tasked with "creating the conditions for economic growth and opportunity," it should prioritize avoiding this outcome.

An effective voluntary pre-clearance/licensing process is critical. The IFR introduced the concept of a pre-clearance/licensing process, which we endorse under the right circumstances, including that it be voluntary. A voluntary pre-clearance/licensing process must have clear guidelines and efficient administration in order to provide the clarity necessary for companies to comply with the IFR and the certainty required for business dealings. Indeed, this process becomes even more important as most companies want to ensure they are not just minimally compliant, but that all transactions they enter into are clearly and verifiably compliant with the law and will remain in effect and not be invalidated with respect to the ICTS transactions described in the pre-clearance/licensing authorization, notwithstanding any subsequent changes to the regulations. Importantly, the parties US companies conduct business with demand the same certainty and compliance with the law. Not only will a voluntary pre-clearance/licensing process allow for more certainty in the business community, it will 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.

The voluntary pre-clearance/licensing process should include the following elements:

- **Guidance on what transactions create national security risk that would potentially benefit from review under a voluntary pre-clearance/licensing process.** Commerce should put forth criteria by which parties can judge the relative risk of a particular transaction. At present, there is no compliance guidance for companies to build programs or judge the risk of any particular ICTS transaction.
- **Use of the pre-clearance/licensing process should be voluntary and structured in the least burdensome way to address risk**. **A mandatory or compulsory process will grind commerce to a halt resulting in severe disruption to the economy.** A pre-clearance/licensing process

should be voluntary and made available to companies who seek greater certainty about the permissibility of a particular transaction, especially with regard to whether a transaction can proceed without mitigation, or otherwise understand what mitigations would be necessary to move forward. The process should also be made available to broad types or categories of transactions so as to avoid the need for transaction-by-transaction clearances where possible. In addition, the process should allow for the voluntary pre-clearance/licensing of transactions or types of transactions that encompass multiple covered technologies or risks.

- **Commerce must be adequately resourced to carry out the voluntary pre-clearance/licensing process.** As we pointed out in our comments in response to the IFR, 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 pre-clearance/licensing requests. We urge Commerce to identify a lead agency or bureau to coordinate the implementation of this rule and associated voluntary pre-clearance/licensing process. 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.
- **Commerce's period for review should be time-bound by regulation.** There should be a presumption of approval and a safe harbor for the transaction if Commerce does not affirmatively issue an additional request for information within 30 calendar days. Any longer time period will be detrimental to U.S. competitiveness. The 30 day review period should not result in an automatic extension/request for additional information. Commerce must allocate sufficient resources to conduct meaningful, expeditious, and sufficient reviews.
- **The voluntary pre-clearance/licensing process should only require minimal data points.** Such an approach could take the form of a short-form declaration that includes the parties to the transaction, contact information, description of item/service that is the subject of the transaction, brief description of its end use, and any information the company wishes to provide regarding risk mitigation. Requiring parties to provide more information will be overly burdensome. Data elements that do not directly relate to risk assessment should not be required (ECCN, HTS, value, etc).
- **The voluntary pre-clearance/licensing process should allow Commerce to make public the names of foreign entities whose goods and services are the subject of an approved or denied Commerce pre-clearance/license.** Publicly stating which entities are subject to voluntary pre-clearance/licensing, whether approved or denied, would help to generate awareness and provide helpful information for other U.S. companies considering transactions with such entities. Confidentiality protections should be included, and the name of the US entity that sought the license should not be published.
- **The voluntary pre-clearance/licensing process should result in the publication of categories of pre-cleared ICTS transactions that do not warrant scrutiny under the rule.** At present, it is not at all clear which categories of transactions are considered to be higher-risk and which present minimal risk. In order for the voluntary pre-clearance/licensing process to be at all functional more information about which categories, types or classes of transactions are within scope needs to be made available to companies so they can make informed decisions about whether and when to seek pre-clearance/licensing determinations.

Specific Questions

1) *Given the differences between the type of transactions subject to CFIUS jurisdiction, those governed by BIS's export control regime, and ICTS Transactions governed by the interim final rule, are the CFIUS and BIS processes useful models for an ICTS Transaction licensing or pre-clearance process? If so, are there specific factors or aspects of the CFIUS and BIS processes that Commerce should consider?*

Given the continued lack of clarity surrounding the specific types of ICTS Transactions that will be subject to this rulemaking, it is not clear to us that the premise of this question is, in fact, accurate. Indeed, while the IFR states that Transactions actively undergoing CFIUS review will not be subject to the IFR, it does not go much further than that, and in fact seems to hold the door open to sweeping in other types of investment transactions (*i.e.,* the "types" of transactions that CFIUS reviews). The IFR also does not explicitly mention how the IFR interacts with the Export Administration Regulations (EAR), nor is it clear whether exports subject to the EAR are considered ICTS Transactions that would simultaneously be subject to the IFR. In fact, the broad definition of "transactions" within the EO and IFR does not clearly preclude either investment or export transactions from being swept up by the rule.

However, to the extent ICTS Transactions are substantially different from those captured under CFIUS and the EAR, there are aspects of both processes that provide a potentially useful launching point for the development of a voluntary pre-clearance/licensing process. At the highest level, both regimes balance the need for commercial certainty with national security considerations in a way that the current IFR does not. There are several ways in which both CFIUS and the BIS process enshrined in the EAR offer useful models for Commerce to consider as it seeks to build out a voluntary pre-clearance/licensing process.

Safe harbor. The CFIUS rules include a "safe harbor" for investments through which a foreign person acquires less than 10% equity in a U.S. business through a passive investment.[1] A similar "safe harbor" would be useful in this context. This approach is consistent with the IFR itself, which requires Commerce to identify a subset of ICTS transactions that would require evaluation. Where CFIUS jurisdiction is triggered, the CFIUS regulations also give parties flexibility relative to how to notify CFIUS of a relevant transaction. Parties to a foreign investment in the United States may submit a short-form declaration, triggering a 30-day assessment period,[2] or they may submit a Joint Voluntary Notice to trigger a more robust 45-day review period that may be followed by an additional 45-day investigation period (as needed). Once CFIUS completes its review, parties generally have safe harbor from further investigative action, which allows for confidence in closing deals and otherwise operating in the marketplace.[3] That being said, it may make sense that parties to transactions that meet certain non-substantive criteria (*e.g.,* in IFR subparagraphs (a)(1)-(3) of Section 7.3 (*i.e.*, transactions subject to U.S. jurisdiction, involving property in which a foreign country or a national thereof has an interest, initiated, pending, or completed after a specified date)) be able to submit notice to Commerce of such transactions. If Commerce does not initiate an evaluation of that

[1] 31 C.F.R. § 800.302(b).
[2] 31 C.F.R. § 800.402.
[3] 31 C.F.R. § 800.508

transaction within a specified period (*e.g.*, 30 days) then the parties should be assured that they can proceed with the transaction without fear of subsequent government scrutiny. The safe harbor should also remain in place for the specific ICTS Transaction described in the original notice. We also recommend that transactions wherein risk-mitigating technologies and/or other non-technological best practices have been applied be eligible for safe harbor – or alternatively, expedited pre-clearance/licensing.

Mitigations. The CFIUS regulations, in connection with their governing statute, provide an opportunity for the parties to a covered transaction and the U.S. government to agree to certain measures intended to mitigate the risks to U.S. national security.[4] A similar process in the context of the voluntary pre-clearance/licensing process would be useful. The criticality assessment conducted by DHS pursuant to the same EO that gave rise to the IFR could provide an approach for identifying the types of ICTS transactions that may be subject to mitigation (*i.e.,* "manageably critical"), and for identifying the types of ICTS transactions that do not require mitigation because they do not create a national security risk (*i.e.,* "not critical"). We recommend that Commerce work with DHS to better understand the mechanics of DHS' criticality assessment and if found to be a viable model, ensure DHS is able to update the assessment to support consideration of mitigations. Adoption of technology-enabled and/or other non-technological best practices should also be considered acceptable mitigation.

2) *Pre-clearance or licensing processes can take a range of forms from, for example, a regime that would require authorization prior to engaging in an ICTS Transaction, to one that allows entities to seek additional certainty from the Department that a potential ICTS Transaction would not be prohibited by the process under the interim final rule. What are the benefits and disadvantages of these various approaches? Which would be most appropriate given the nature of ICTS transactions? How can these approaches be implemented to ensure that national security is protected?*

Any process that is developed should be voluntary in nature. No regime should *require* authorization prior to engaging in an ICTS Transaction. In the case of this IFR, requiring pre-authorization would be nearly impossible because of the scope of covered transactions. The time it would take to review every single ICTS Transaction that falls under this rule would be prohibitive to business, and further would not achieve any discernible purpose given every single ICTS Transaction captured under the IFR cannot possibly pose a national security risk. The number of transactions in play, coupled with the resources it would take for Commerce to review all of these transactions, would make such a process unwieldly, if not nearly impossible to undertake. Beyond that, the resources it would take for companies to actually comply with a process that requires pre-authorization would be vast, ultimately serving to undermine U.S. competitiveness.

As such, we recommend that Commerce seek to build a voluntary pre-clearance/licensing process founded on a "presumption of approval" – or put another way, that ICTS Transactions should be

[4] *See* 50 U.S.C § 4565(1)(3)(A)(i); 31 C.F.R § 800.101(a). Likewise, under the EAR Commerce may issue a license for a transaction subject to certain limitations or conditions. *See* 15 C.F.R § 736.2(b)(9) (prohibiting the violation of terms or conditions of a license issued under the EAR); *id.* at § 750.7(a) (defining the scope of activity authorized under a license "[u]nless limited by a condition set out in a license."

considered as not in scope of the ICTS review regime unless and until Commerce flags a certain transaction or class of transaction as creating a national security concern so as to warrant further Commerce review, and effectively provides notice of such to impacted parties to such transactions. As we recommended above in the "Safe Harbor" section, if Commerce does not initiate an evaluation of that transaction within a specified period (*e.g.*, 30 days) then the voluntary pre-clearance/license application should be deemed approved and parties should have the confidence to move forward with the transaction.

Whereas aspects of the BIS process are built upon a presumption of denial – i.e. an application for a license to export to a named Entity will likely be denied – such a process would not work here. Because there is not a narrow set of companies outlined in the IFR nor a clear list of transactions that the USG considers to be high-risk, the scope of transactions swept up by the IFR makes such an approach untenable. We instead suggest that Commerce consider creating a mechanism similar to the General License under the EAR, which provides a broad grant of authority to exporters for certain categories of products.

3) *Are there categories or types of ICTS Transactions described in 15 CFR 7.3 or within the interim final rule that should or should not be considered for a license or preclearance? Are there categories or types of ICTS Transactions described in 15 CFR 7.3 or within the interim final rule that the Department should prioritize for licensing or pre-clearance? Should the licensing or pre-clearance process be structured differently for distinct categories or types of ICTS Transactions?*

As we mention above, we encourage Commerce to build a process based upon a "presumption of approval," or a presumption that certain ICTS transactions or classes of transactions are not within the scope of the ICTS review regime established by the rule, especially given the breadth of its scope as written. Based on the definitions included in the IFR[5], it would appear 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 country designated as a foreign adversary, could trigger a review under the rule. The broad review regime established by the IFR seemingly extends to transactions that do not create any risks at all. Including a review of all transactions where there is simply a "foreign interest" is overbroad. As such, it is imperative that as a part of the development of the licensing process, Commerce develop a list of transactions that implicate a specific, identified risk, as all transactions with a foreign partner are not inherently risky. Additionally, if Commerce does not limit the scope in the course of the development of the licensing process, it risks actually missing transactions that pose legitimate national security risks given the overwhelming amount of pre-clearance/licensing requests it will likely receive.

Commerce, and the USG more broadly, needs to determine a way to identify specific categories of transactions that pose a potential national security risk, and therefore should be considered for voluntary pre-clearance/licensing. The burden should fall on the USG to articulate why certain transactions are problematic, instead of leaving it to industry to guess as to what national security

[5] See Interim Final Rule §7.3(a), which 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.

risk the USG is trying to address by placing things like "desktop applications, mobile applications, and gaming applications used by over one million U.S. persons" on the list of covered transactions (as one example).

Once Commerce has established a scheme based on objective criteria and in fact applied that scheme/criteria so as to identify those transactions that pose significant risks to national security (including, specifically, an identification of problematic counterparties to those transactions), Commerce could meaningfully prioritize a review of such identified high-risk transactions in the voluntary pre-clearance/licensing process. Pending the further development and articulation of the underlying ICTS review regime, we anticipate there might also be transactions or classes of transactions that should not be considered for pre-clearance/licensing, as they would be out of scope given the lack of nexus to a significant national security concern, and thus deemed "pre-approved" as stated above. Such an approach would also help address the resource concern we have raised on several occasions, alleviating the burden that would be associated with Commerce needing to review an overwhelming number of transactions submitted for voluntary pre-clearance/licensing by companies seeking to meaningfully comply but also trying to avoid the extreme uncertainty generated by the rule. Again, we reiterate that once risks have been identified, companies with risk mitigating best practices in place – both technology-based and non-technology-based – should have safe harbor from both the voluntary pre-clearance/licensing and subsequent review processes, or should get a near automated or expedited pre-clearance/licensing decision.

We also discourage Commerce from capturing ICTS Transactions involving a company's employees, regardless of their location, or intracompany transfers under the voluntary pre-clearance/license process. This type of transaction, which is ostensibly captured under the IFR as currently written, is a part of day-to-day business operations and does not implicate national security. Addtionally, the national security concern implicated with foreign national employees is already addressed with deemed export rules.

4) *Should a license or pre-clearance apply to more than a single ICTS Transaction? For example, should the Department consider issuing a license that applies to multiple ICTS Transactions from a single entity that is engaged in a long-term contract for ICTS? If so, what factors should the Department evaluate in determining the appropriateness of such a license or series of licenses?*

Yes, we believe that a license or pre-clearance should apply to more than a single ICTS Transaction and should also cover factually similar transactions. Allowing a license or pre-clearance to apply to more than one ICTS Transaction, particularly those that may be undertaken under a long-term contract, would help to make the process less onerous and more efficient. When a review has been completed, or a license granted, it should be broad enough to cover an entire contract and not require piecemeal approvals for each element of technology in the involved deal. As referenced above, a mechanism similar to the General License granted to exporters under the EAR would potentially offer a useful way to add certainty to the pre-clearance/licensing process.

One potential approach worth considering is to view a long-term contract (LTC) as a single ICTS Transaction. In cases where a LTC raises security concerns based upon the objective criteria that Commerce uses to assess transactions, the LTC should delineate the items involved. A blanket Purchase Order (PO) or basic ordering agreement/general terms agreement that merely sets basic

terms and conditions to apply to subsequent PO releases would not be considered an eligible long-term contract in that situation given the lack of specificity included therein, but in circumstances where there are not concrete, identified risks, it should be sufficient. To be clear, this type of consideration would be in addition to, and not a substitute fo,r pre-clearance for broad categories or types of transactions, as described above on page 3.

Commerce should also consider establishing a "trusted importer" program for the purposes of ICTS import transactions. Commerce should consider participation in the C-TPAT program and the company's compliance record for the purposes of participation in the "trusted importer" program. Trusted Importers should receive blanket authorizations for relevant import transactions for at least 3 years.

5) *What categories of information should the Department require or not require, e.g. technical, security, operational information?*

It is difficult to provide input on this question when there is no clarity regarding what transactions are in scope of the broader review scheme established by the rule and the applicable national security risks the rule is trying to address. Technical information provided should focus on the extent to which the ICTS in question is capable of two-way communications between the devices and agents of the foreign adversary. Any proprietary information should be disclosed in a way that precludes the possibility of third-parties accessing or seeing that data.

6) *While the Department understands that business decisions must often be made within tight timeframes, the Department may not be able to determine whether a particular ICTS Transaction qualifies for a license or pre-clearance without detailed information and analysis. Considering this tension, should the Department issue decisions on a shorter timeframe if that could result in fewer licenses or pre-clearances being granted, or would the inconvenience of a longer timeframe for review be outweighed by the potential for a greater number of licenses or pre-clearances being issued?*

We disagree with the premise of the question, which suggests Commerce may well face a tradeoff between thorough reviews of licensing/pre-clearance applications and shorter, efficient reviews of a potentially large number of applications. This is a false dichotomy, as Commerce should make sure it has the appropriate resources in place to meet the workload that is likely to flow from the IFR, and structure the IFR and the voluntary licensing/pre-clearance process accordingly. Doing so will allow for speedy review of a significant number of pre-clearance/license requests and therefore allow Commerce to avoid having to make a choice between issuing fewer pre-clearance/licenses in a shorter timeframe or greater number of pre-clearance/licenses over a longer timeframe.

We offer additional comments related to the timeframes described in the IFR. The IFR indicates that the pre-clearance/licensing process would allow parties to proceed with a transaction if Commerce has not raised objections within 120 days. This is not a commercially reasonable timeframe. We believe that 30 days will give the government ample opportunity to decide if additional information is required to assess risks associated with a transaction. If the government wants to request more time after an initial review because something related to the deal under review has raised concerns, then it could go back to the company and indicate the existence of such. In the ordinary course, 30 days should be more than enough time to ascertain whether or not there is likely to be an issue

requiring "detailed information and analysis," which could then be undertaken in a further review. However, the 30 day review period should not result in an automatic extension/request for additional information. Commerce must allocate sufficient resources to conduct meaningful and sufficient reviews.

In any case, we recommend that Commerce maintain the option for a company to obtain an emergency pre-clearance or license. This may be another instance in which it is helpful to look to the EAR, which lays out a process for a company to seek "emergency processing" of a license and which states that BIS will attempt to expedite evaluation when it judges the circumstances warrant such expedition.[6]

7) *How should the potential for mitigation of an ICTS Transaction be assessed in considering whether to grant a license or pre-clearance for that transaction?*

It is somewhat difficult to answer this question, as we believe that, in the first instance, a more fundamental step needs to occur: figuring out which of those transactions listed in the IFR actually present a legitimate national security risk and therefore require evaluation and/or additional attention.

As we referenced in our comments to the IFR, Commerce should leverage an updated version of the DHS/CISA criticality assessment that incorporates meaningful industry input as a way to narrow the scope of the IFR, but also as a means to understand which sorts of transactions present risks that are mitigatable.[7] Although it requires updating, the DHS/CISA criticality assessment does provide helpful criticality levels, which includes "manageably critical" as one of the levels, meaning that "compromise of the element could potentially have significant regional or national impacts, including affecting the confidentiality, integrity, or availability of data or the system, *but risks can be mitigated* (emphasis added) with reliable and reasonable measures when properly implemented, such as using encryption or having redundant components supplied by multiple vendors and manufacturers." Those elements that are considered "manageably critical" could be used by Commerce in determining whether the risks associated with a transaction can be mitigated.

We also noted in our initial comments to the NPRM that there are multiple ways in which risks that may occur within transactions can be reasonably mitigated. Industry is constantly innovating to address the dynamic threat environment and those innovations that support risk management efforts can and should be taken into account when assessing whether the risk that emanates from particular transactions can be mitigated. Commerce could again potentially consider a company's adherence to certain risk-management standards or principles as mitigating factors, if not exempt such transactions altogether if they adhere to such standards. Standards to consider as potentially mitigating include those laid out in the NIST Cybersecurity Framework, the ISO/IEC 27000 series, and standards compiled by the ICT Supply Chain Risk Management Task Force.[8] Commerce can also

[6] 15 CFR §748.4.
[7] https://www.cisa.gov/publication/ict-eo-13873-response
[8] See Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report (September 2019).

incentivize adoption of technologies that strengthen supply chain security by making such adoption a factor in eligibility for a safe harbor and/or pre-clearance/licensing.

8) *If a license or pre-clearance request is approved, but the subject ICTS Transaction is subsequently modified, what process should be enacted to avoid invalidation of the license or other form of pre-clearance?*

If the ICTS Transaction is modified following approval/issuance of pre-clearance or license, the party should notify Commerce of modification and provide updated information on the nature of the modification, how it changes the transaction, and additional information relevant as to why the transaction should be fine to proceed. Transaction modifications involving changes to the item that do not affect functionality (meaning modifications that affect form or fit only) should be acceptable under the existing pre-clearance/license approval. There should be an expedited way for parties to affirm that no additional risk has been introduced due to any changes in the transaction, and/or that any risk mitigating technologies or standards remain in place.

9) *Should holders of an ICTS Transaction license or other form or pre-clearance have the opportunity to renew them rather than reapplying? If so, what factors should be considered in a renewal assessment? What would be the appropriate length of time between renewals? How should any renewal process be structured?*

This question seems to presuppose that a time limit is necessary, but it is not clear to us that it is. Once a transaction is pre-cleared and/or approved, it should be cleared and/or approved for the duration, unless specifically mitigated by a license condition for a specific reason. Therefore, we encourage Commerce to reconsider whether a time limit is actually necessary.

Perhaps a more reasonable way for Commerce to approach the question of renewals would be to detail circumstances where a pre-clearance/license is no longer valid, but a company should not have to proactively renew if the transaction type in question was cleared previously (*i.e.* Commerce did not find any national security risks).

However, in the event that Commerce decides a time limit is warranted, we encourage licenses and/or pre-clearances to be valid for the longest possible period of time (in any event, no less than a period of ten years) and be eligible for renewal through an expedited process. Factors to consider include a company's continued adherence to international standards/best practices, adoption of risk-mitigating technologies, and level of risk associated with the transaction.

***

ITI appreciates the opportunity to submit comments in response to this ANPRM. It is imperative that industry and government work together to achieve the trusted, secure, and reliable global ICT 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 narrowly tailor the existing IFR and additionally structure a clear, voluntary pre-clearance/licensing process will help to provide much needed certainty to businesses, strengthen our collective security, and allow for continued U.S. technological leadership and competitiveness.

The way in which the voluntary pre-clearance/licensing process is structured is absolutely critical to all ITI member companies. As such, we strongly encourage Commerce to continue to engage with stakeholders not only as it seeks to develop the process, but as it seeks to carry forth the IFR more generally. We look forward to continuing to work with Commerce as it further narrows the IFR and the associated pre-clearance/licensings process. Please 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