CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

NEIL L. BRADLEY
EXECUTIVE VICE PRESIDENT &
CHIEF POLICY OFFICER

CHRISTOPHER D. ROBERTI
CHIEF OF STAFF
SENIOR VICE PRESIDENT,
CYBER, INTELLIGENCE, AND
SECURITY POLICY

March 22, 2021

The Honorable Gina Raimondo
Secretary
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Re: Securing the Information and Communications Technology and Services Supply Chain; 86 FR 4909; Docket No. DOC-2019-0005; RIN: 0605-AA51

Dear Secretary Raimondo:

The U.S. Chamber of Commerce (Chamber) is submitting this letter in response to the U.S. Department of Commerce's (Department) request for comment on the interim final rule (IFR or Rule) to implement provisions of Executive Order 13873 (EO), *Securing the Information and Communications Technology and Services (ICTS) Supply Chain*.

The Chamber has deep concerns with the IFR. While it appears that the Department considered concerns raised by many stakeholders and entities that would be impacted by the rule, the parameters of the underlying EO limited the Department's ability to resolve its significant shortcomings. Accordingly, the current IFR on which we are commenting remains highly problematic.

In particular, and as outlined more fully below, the IFR: (1) will provide limited actual protection to stop malicious actors; (2) requires compliance programs that are unrealistic to implement; and (3) will impose enormous costs on the private sector – many of which are not fully accounted for in the rule. The Department's Regulatory Impact Analysis & Final Regulatory Flexibility Analysis (RIA) includes extremely troubling observations such as "the workload for enforcement for this…executive order is unprecedented,"[1] "small firms may find it difficult to remain viable [due to the rule],"[2] and "even those who did not engage in a transaction affected by the Rule, may face higher production costs" that underline our concerns.[3]

While the RIA states "the benefits of this Rule are significant…and would likely outweigh the costs associated with the Rule" the Department does not quantify these benefits – but it does quantify the Rule's significant costs.[4] Cumulatively, this reinforces our contention that the IFR will be more harmful than helpful in advancing its stated policy objective – to secure the ICTS supply

[1] U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain (RIN 0605-AA51), Regulatory Impact Analysis & Final Regulatory Flexibility Analysis. p. 9
[2] Ibid. p. 33
[3] Ibid. p. 21
[4] Ibid. p. 26

chain. Accordingly, the Department should be able to point to specific benefits to justify imposing these costs on the private sector.

Further, the Department's announcement on March 17 that it had subpoenaed multiple Chinese companies points to a slightly different focus than what is articulated under the rule.[5] Specifically, this action appears to target companies acting with intent to subvert U.S. national security – not against problematic transactions. The Department should clarify *who* and *what* it is targeting and make that clear in the final Rule.

Implementation of this rule also undermines the purpose of the methodical and comprehensive one year review of the information and communications technology (ICT) industrial base that your department will conduct with the Department of Homeland Security pursuant to President Biden's *Securing America's Supply Chains* Executive Order (Supply Chain EO).[6] This review should be allowed to conclude before implementing this highly problematic IFR, which was conceived and drafted under the previous administration.

Getting ICTS security right is a shared goal of industry and the administration. The U.S. Cyberspace Solarium Commission[7] (Commission) determined that whoever holds the keys to ICTS "holds the keys to the next 20 years of innovation and economic growth and prosperity."[8] Over the past two decades, foreign adversaries have mobilized to secure a dominant position in the ICTS market through a concerted, strategic effort, while the U.S., according to the Commission, has relied on a "disparate, largely disconnected [series of] actions, including [EO 13873]."[9] The U.S. needs to account for the sophisticated and coordinated approach that many foreign adversaries are pursuing to dominate the ICTS market – and act strategically in providing the tools necessary to help the U.S. and the business community compete in this new reality. This IFR, unfortunately, does not do that.

For these reasons and the reasons articulated below, we urge the Biden Administration to suspend this rule. If the Administration is unwilling to suspend this rule, then at a minimum, the Department should adopt the recommendations outlined in our appendix to provide important clarity to various aspects of the rule. Our concerns are discussed below and in the attached appendix.

The Rule Will Provide Limited Benefits to Stop Malicious Actors

The Trump administration issued EO 13873 in response to growing threats of malicious actors seeking to create and exploit vulnerabilities in ICTS infrastructure. The RIA justifies the IFR because: (1) private parties engaging in ICTS transactions with foreign parties…may lack the information, expertise, or incentive to evaluate and internalize the potential National Security risks

---

[5] U.S. Secretary of Commerce Gina Raimondo Statement on Actions Taken Under ICTS Supply Chain Executive Order, March 17, 2021. https://www.commerce.gov/news/press-releases/2021/03/us-secretary-commerce-gina-raimondo-statement-actions-taken-under-icts

[6] Executive Order 14017, "America's Supply Chains." Sec. 4(iii). February 24, 2021. 86 FR 11849.

[7] The Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The CSC was led by Sen. Angus King (I-ME) and Rep. Mike Gallagher (R-WI). The CSC had 10 commissioners, including 4 legislators and 6 nationally recognized experts from outside of government.

[8] Cyberspace Solarium Commission, "Building a Trusted ICT Supply Chain, CSC White Paper #4." p. ii, October 2020. https://drive.google.com/file/d/1efo96fPx5WkOxTiFFY1r5y3lFqdit00C/view

[9] *Ibid.* p. ii., see endnote 4.

involved in ICTS transactions with foreign parties; (2) private parties may in fact not disclose suspect suppliers or supplier behavior out of fear of putting themselves or others at risk, legally, from governments or other private entities; and (3) the market may not provide an optimal solution to the potential risk and harm to the ICTS supply chain.[10] These justifications simplify enormous complexities in ICTS management and place undue confidence in the IFR.

ICTS Supply Chains Are Complex

The inputs for ICTS originate from a variety of sources across the globe. This results in complex, interconnected, and globally distributed supply chains that can include multiple tiers of suppliers, which makes it difficult for industry and government to understand and control how ICTS applications are acquired, developed, distributed, and deployed through multi-layered supply chains.

Typically, a business or federal agency acquiring an ICTS application may only know about the participants directly connected to it in the supply chain, sometimes called a first-tier supplier. But first-tier suppliers may rely upon other suppliers to obtain various equipment, software, or services through various means, including reusing existing equipment or legacy software; outsourcing system development to an additional supplier; developing the capability in-house; or acquiring the capability directly from a supplier or commercial off-the-shelf vendor.

In addition, corporate structures present their own challenges. In some cases, a parent company (or subsidiary) may own or control companies that conduct business under different names in multiple countries. This can present further challenges to businesses or federal agencies seeking to understand the source of an ICTS product and its potential vulnerabilities.

While many businesses maintain compliance programs to track supplier integrity there is an increasing recognition that supply chain security requires the U.S. government to inform the private sector of emerging threats and vulnerabilities. The increasing sophistication and prowess of many malicious actors – especially those efforts supported by foreign governments – means that it will become increasingly challenging for even the most committed businesses to understand and anticipate emerging threats without the support of the U.S. government.

Rule Not Coordinated with Other Federal Efforts to Protect Supply Chains

Adding to this complexity for the business community are the numerous efforts by the federal government and private sector to promote ICTS supply chain security. This rule would join a variety of supply chain security efforts, led by the government and the private sector.

The federal government's initiatives include a wide range of strategies, task forces, advisory committees, and programs to understand and mitigate supply chain risks, including: the Department of Commerce's Bureau of Industry and Security's Entity List; the Department of Homeland Security's Information and Communications Technology Supply Chain Risk Management Task Force; the President's National Security Telecommunications Advisory Committee; the Department of Defense's Cybersecurity Maturity Model Certification (CMMC); the Department of State's Clean Network program; the Director of National Intelligence's Supply Chain and Counterintelligence

[10] U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain (RIN 0605-AA51), Regulatory Impact Analysis & Final Regulatory Flexibility Analysis. p. 2-3.

Risk Management Task Force;[11] the National Institute of Standards and Technology (NIST) Cyber Supply Chain Risk Management (C-SCRM) program; the Federal Communications Commission's efforts to prohibit the use of federal subsidies to purchase equipment or services deemed to pose national security risks and to fund replacements; the Department of Treasury's Office of Foreign Assets Control; the Office of Management and Budget's Federal Acquisition Security Council; the interagency Committee on Foreign Investment in the United States (CFIUS), and the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector's (formerly known as "Team Telecom" prior to its formalization pursuant to Executive Order 13913) transaction review programs.

While the Department clarified that the IFR does not apply to transactions under review by CFIUS, numerous other federal efforts and programs remain, and the potential overlap and coordination challenges introduce a significant – and likely untenable – compliance burden. It also reinforces our concern that the IFR only adds to the numerous strategies and "number one" priorities of the federal government's supply chain security efforts. Based on the IFR's limited recognition of other activities to prevent malicious behavior, it's not clear how this rule will help the private sector focus resources on supply chain security when it is instead focusing on the many efforts across the federal government – and especially with this rule – that do not fully coordinate with each other.

"Foreign Adversaries" Definition Provides Limited Benefit

One of the many problematic aspects of the rule is the definition of "foreign adversaries." We are grateful that the Department included a provision that determines how foreign adversaries are identified, but listing China, Cuba, Iran, North Korea, Russia, and the Maduro regime as foreign adversaries provides false comfort to businesses and will undermine efforts to prevent ICTS supply chain attacks because it does not take into account the realities and complexities of modern manufacturing processes and supply chains.

More importantly, this aspect of the rule undermines a central goal to "protect our country against critical national security threats." A business complying with the rule is still at risk of a malicious action by a foreign adversary. There is little evidence that a malicious actor is restricted by geography. To the contrary, determined adversaries will always use every opportunity to advances their interests – anywhere in the world. No company is immune to malicious actors – especially those supported by foreign governments. "Walling off" certain countries from providing ICTS means that foreign adversaries know to concentrate their efforts on facilities outside their borders – which this rule does not address. Vigilance to specific threats, irrespective of geography, is preferable to geography-based barriers.

Projected Benefits of the IFR Are Not Supported By the RIA

The benefits of this rule are not supported by the RIA. Despite the enormous range in compliance costs for the business community, the RIA acknowledges the benefits of the IFR are "incalculable."[12] But rather than providing examples of transactions and other activities that this rule would help stop, the RIA instead points to the various ways malicious actors are exploiting

[11] National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 6306, 133 Stat. 1198 (2019), https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf.
[12] U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain (RIN 0605-AA51), Regulatory Impact Analysis & Final Regulatory Flexibility Analysis. p. 24.

vulnerabilities in the ICTS supply chain and the growing damage those attacks are posing to the ICTS supply chain.

While the Department has powerful tools to investigate suspicious behavior – including the subpoenas survey authority of the Department's Bureau of Industry and Security – the RIA projects only two special agents and one attorney will be assigned to perform these investigations.[13] It is therefore difficult to believe that these investigations will be anything more than modest in number and limited in scope given how difficult these sorts of investigations will be to perform and how many different industry sectors they can impact. There are approximately 4.5 million organizations potentially covered by this rule with potentially millions of transactions each year that are not publicly or widely known and are often covered by contracts intended to protect competitive practices. Indeed, in contrast to the modest staffing assumptions, the RIA recognizes that the "workload for enforcement for this type is unprecedented."[14] Given the limited resources provided by the Department for this IFR, a more narrowly tailored and targeted rule would be more effective at reducing national security risks and would not result in wasting limited resources on low risk transactions.

We agree that eliminating ICT supply chain attacks would result in enormous benefits to the U.S., its businesses, and citizens. However, it is not clear how the limited number of investigations envisioned under the RIA (less than 250 per year) will result in the sort of dramatic improvements to supply chain security, while the uncertainty created by rule will damage impacted entities no matter the approach to enforcement. Additionally, the benefits envisioned by the Rule would not flow from the rule itself. The Department assumes the rule's retroactive approach will be effective in *stopping* problematic ICTS transactions when in reality, the Rule will be reacting to already problematic transactions.

Required Compliance Programs Are Difficult & Unrealistic

Compliance Regime Fails to Recognize Realities of Supply Chain Threats and Contradicts the Department's Assumptions

There is a disconnect between the Department's recognition that "private parties engaging in ICTS transactions with foreign parties…may lack the information [and] expertise…to evaluate and internalize the potential National Security risks involved in ICTS transactions with foreign parties" and the assumption that a compliance plan will be able to overcome these fundamental challenges – especially when malicious actors are often acting to purposely hide their activities.

In order to build a compliance program, businesses need to be able to assess risk of a particular transaction to determine whether to avoid the transaction, license the transaction, etc. The IFR provides no guidance on what should constitute high risk transactions or low risk transactions. Because there is such a broad array of transactions to monitor, it is not realistic for the Department to assume that the private sector will be able to implement a compliance program that can monitor the sheer scope of activities called out under the Rule.

The greatest challenge to companies in complying with this rule is that there is no predicting what transaction the Department will consider is within scope. Without being able to predict what transactions will fall under the rule, companies cannot build compliance into their supply chains and

[13] Ibid. p. 8-9.
[14] Ibid. p. 9.

infrastructures to prevent the risks that the rule is intended to thwart. Rather, the rule takes a retroactive approach in penalizing companies for a broad set of transactions that are later found to be risky.

We believe that the Department is placing unrealistic expectations on the private sector to develop compliance programs with the level of sophistication and perception into supply chains envisioned in the RIA. As discussed above, it is widely reported that foreign adversaries are working strategically to capture the ICTS markets using a variety of efforts including unfair and deceptive trade practices, to include state-led intellectual property theft. The private sector is increasingly operating in an international marketplace that—due to the intervention of foreign adversaries—is neither free nor fair.[15]

The reality is that most businesses – especially small businesses – simply will be unable to build compliance programs to counter the resources of a state-backed malicious actor. The information this rule expects the private sector to collect and maintain is not readily available for even the most sophisticated of entities. It isn't even entirely clear what information Commerce would expect businesses to collect. Given the breadth of the rule simply ruling out any state interests would not be sufficient.

Lack of Federally Recognized ICTS Best Practices Hurts Developing Compliance Programs

While the Department expects the business community to adopt compliance programs to screen for transactions that could pose national security challenges, the lack of guidance regarding how to develop such a program in the rule is problematic. This leaves the business community – especially small businesses – at a disadvantage to understand how to organize a program to help them identify the sorts of transactions that the Department recognizes the business community may be challenged to identify due to a "lack [of] information [and] expertise."[16] While a federal government-recognized set of management "best practices" to protect against ICT supply chain attacks would go a long way towards helping this effort, the federal government presently has done no such thing.[17] This only further hurts the business community's efforts to protect themselves.

Indeed, the IFR does list the sources or information, factors, and other variables related to a transaction that the Secretary may consider when reviewing a transaction. However, the business community cannot develop sound and effective compliance programs because the Department acknowledges that "this list is non-exclusive and does not prevent the Secretary from reviewing any available information."[18]

Concerns with Proposed Licensing Process

We are grateful that the Department accepted our request to developing a licensing process for parties to obtain a pre-approval on potential transactions. While this is a reasonable and appropriate provision in the abstract and we will review the Department's proposal, we are

[15] Cyberspace Solarium Commission, "Building a Trusted ICT Supply Chain, CSC White Paper #4." p. ii, October 2020. https://drive.google.com/file/d/1efo96fPx5WkOxTiFFY1r5y3lFqdit00C/view
[16] U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain (RIN 0605-AA51), Regulatory Impact Analysis & Final Regulatory Flexibility Analysis. p. 2.
[17] U.S. Government Accountability Office, "Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks." December 2020. https://www.gao.gov/assets/gao-21-171.pdf
[18] Section 7.100(a).

concerned that the enormous number of transactions each year and the limited resources the Department is committing to this proposal will limit the ability of this program to review transactions in a timely manner and could ultimately negatively impact efforts at compliance and needlessly delay transactions. Additionally, publishing guidance to identify the types of transactions where businesses should seek a license and what factors Commerce will consider in determining whether to approve or deny a license could help to form a basis for developing compliance. Absent that licensing guidance, there is no opportunity for business to be proactive about compliance with this rule.

The Rule Will Impose Enormous Costs

It is rare that a federal regulatory impact analysis (RIA) cannot identify a satisfactory range of costs and benefits associated with the proposal. The RIA for this IFR includes enormous ranges, from the number of parties impacted – 268,000 to 4,533,000[19] - to the estimated costs – from between $1 billion to $52 billion in the first year and between $95 million to $15 billion in subsequent years.[20] Given this enormous range in costs, it is difficult to fully evaluate the impacts of the rule, particularly because the RIA recognizes that there will be further impacts that it cannot evaluate. This puts businesses in the position of complying with a rule that even the issuing agency acknowledges might create vast and unpredictable compliance costs.

The Department Does Not Include the Full Scope of Costs of the Rule

The RIA anticipated multiple additional costs that it did not attempt to enumerate – but suggested would impose significant harm, including (1) the "restriction of imports from adversarial nations will likely increase production costs" for many firms; (2) "the loss of producer profits and lower profits…of an entire industry subject to a designated transaction;" (3) "even those which did not engage in transactions affected by the Rule, may face higher production costs;" (4) "the impacts of the Rule are not confined to the firms in the industries that produce the products subject to the Rule; (5) "investors will likely take extra time…result[ing] in delays…[that] could impose costs on consumers; and (6) "higher prices and lower consumer and producer surplus is likely to arise among many inter-related industries." [21]

What is clear from this accounting is that the Department recognizes this rule will result in harmful reverberations across the economy, hurting consumers, investors, and businesses. Allowing this rule to go forward without fully accounting for these costs – or seeking to identify appropriate alternatives is another reason the rule should be suspended.

Small Businesses Will Be Disproportionately Hurt By this Rule

The small business community will be hard hit by this rule. Indeed, it appears the small business community will bear all the costs of this rule with little benefit. Specifically, the Department recognizes that "small entities are less likely to have the resources to develop and implement a compliance plan" which is required under this rule but will still need to be in compliance with the rule regardless.[22] Of further concern is the Department's recognition that small businesses "may not

[19] U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain (RIN 0605-AA51), Regulatory Impact Analysis & Final Regulatory Flexibility Analysis. p. 7
[20] Ibid. p. 17
[21] Ibid. pgs. 18-23.
[22] Ibid. p. 30.

have the same ability to deal with the burdens associated with the Rule." The RIA goes on to recognize that: "Faced with the various costs associated with compliance, firms will either have to absorb those costs and/or pass them along to their consumers in the form of higher process. …[D]ue to their lack of market power and their lower profit margins, small firms may find it difficult to pursue either of both of those responses while remaining viable."[23] In either situation, the Department has put the small business community in an untenable position.

Conclusion

Thank you for the opportunity to comment on the Department's proposal. While our members share the Administration's priority to secure ICTS transactions, this IFR from the previous administration continues to be extremely problematic and provides the Secretary with significant authority to intervene in, block, and unwind essentially *any* ICTS transaction, with little to no accountability, transparency, or coordination with other government programs. As the Rule's regulatory impact analysis illustrates, it will result in significant harm to the U.S. economy, businesses, and consumers without a demonstrated national security benefit exceeding its costs. We look forward to continuing to work with the Department—and other federal agencies—to help solve the critical challenges in securing the supply chain.

Sincerely,

Neil L. Bradley

Christopher D. Roberti

Attachment

[23] Ibid. p. 33.