



Office of the Vice President  
Government and Regulatory Affairs

600 14<sup>th</sup> Street, N.W., Suite 300  
Washington, D.C. 20005

March 22, 2021

Mr. Henry Young  
Senior Technology Policy Officer  
Office of the 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. 210113-0009; RIN: 0605-AA51**

Dear Mr. Young:

IBM hereby submits the following comments on the Commerce Department's interim final rule to implement Executive Order 13873, *Securing the Information and Communications Technology and Services (ICTS) Supply Chain*.

IBM shares the U.S. government's objective to improve security in the information and communications technology products and services ("ICTS") supply chain. IBM takes great strides to ensure a secure ICTS supply chain both for ourselves and for our clients. We appreciate and support thoughtful government approaches to national security, such as the Biden Administration's recent Executive Order, *Securing America's Supply Chains*, which calls for a comprehensive review of U.S. supply chains, including the ICTS supply chain, to develop strategic long-term solutions that protect against threats from our adversaries.

This interim rule, however, does not accomplish this goal and remains highly problematic. Despite stakeholder input in the rulemaking process, the resulting interim rule is overly broad, does not provide notice of what is prohibited, and, if implemented, will harm the U.S. economy, fail to enhance national security, and violate principles of due process. The Commerce Department itself estimates in its *Regulatory Impact Analysis & Final Regulatory Flexibility Analysis* ("RIA") that the rule will cost U.S. industry billions of dollars to implement, will have a significant impact on the digital economy, and has elusory benefits that are not quantifiable. For these reasons, the best path forward is to suspend the interim rule and to pursue ICTS supply chain security via the Administration's supply chain initiative, which provides for the Department, together with the Department of Homeland Security, to conduct a comprehensive assessment of the ICTS supply chain in order to develop pragmatic solutions that address identified risks and enhance national security.

We provide the following brief comments on the interim rule and incorporate by reference our previous comments on the proposed rule (provided separately for ease of reference), which remain relevant and largely unaddressed by the interim rule.

### **The Interim Rule Remains Massively Overbroad**

The interim rule remains overly broad, as it grants the Secretary of Commerce wide discretion to prohibit or restrict “ICTS transactions” involving a “foreign adversary” that pose “undue” or “unacceptable risk” to U.S. national security. These terms remain either undefined or defined so broadly that the rule continues to subject billions of dollars of legitimate U.S. commerce to vague and arbitrary government regulation. For example, the interim rule’s all-encompassing and non-exhaustive list of in-scope products and services captures most, if not all, ICTS products and services, leaving U.S. companies with a high level of uncertainty about what transactions could be problematic and where to focus attention. Similarly, the criteria for determining whether a particular transaction poses an undue or unacceptable national security risk remain broad and include a seemingly limitless catchall for any information that the Secretary deems relevant. This leaves U.S. companies to guess which ICTS transactions create an undue or unacceptable national security risk, and, more importantly, what to do about it. Such ambiguity not only makes this rule impractical to implement, but also will result in inconsistent, and possibly counterproductive, implementation across industry, undermining the rule’s very objective to enhance national security. Finally, while we appreciate Commerce’s attempt to clarify the scope of the rule by naming six foreign adversaries (five foreign governments and one foreign person/regime), this does little to clarify the scope or intent of the rule. Because the rule covers ICTS transactions with any person subject to the jurisdiction of a foreign adversary, the rule potentially could prohibit nearly any ICTS transaction with any entity in the named jurisdictions – including legitimate transactions between a U.S. parent company and its subsidiaries in those countries. Moreover, the interim rule continues to define foreign adversary broadly, and grants the Secretary discretion to designate a new foreign adversary at any time. This country-based approach, together with the vague definition of undue or unacceptable risk, inevitably will be overly inclusive of low risk ICTS transactions, cause U.S. companies to abstain from innumerable transactions that present no national security threat and undermine U.S. global competitiveness.

### **The Interim Rule Will Cause Economic Harm Without Achieving its Intended Benefit**

The interim rule creates a costly contingent risk for nearly any transaction involving ICTS, and by the Department’s own calculation, will cost U.S. companies billions of dollars to comply. Imposing these costs on the U.S. economy without a clear and documented benefit to U.S. national security is unwise. The expansive scope of the interim rule grants the government unprecedented authority to review and potentially prohibit, restrict, or unwind legitimate U.S. economic activity that poses an undefined national security threat. Because the rule can apply to almost any ICTS transaction and because undue or unacceptable risk is not well defined, the rule potentially impacts billions of dollars of transactions and creates great uncertainty for a large segment of U.S. business. Due to this uncertainty, many U.S. businesses may avoid otherwise legitimate transactions, impacting the U.S. economy and hampering U.S. innovation.

Furthermore, the Commerce Department's RIA suggests that, in addition to imposing significant compliance costs, the rule also could cause additional economic harm, such as increased production costs due to restricted imports, lower producer profits, and higher costs overall for U.S. companies and U.S. consumers. The RIA estimates a wide range of substantial costs on U.S. business, but acknowledges that the benefits of the rule are "incalculable." While the economic harm of this interim rule is known, the benefit is not so clear.

### **The Interim Rule Fails to Enhance National Security**

The interim rule fails to strengthen ICTS supply chains because it remains so overly broad and vague that it is impracticable for U.S. companies to implement it uniformly. Without more clarity about proscribed behavior, companies are left to guess what constitutes a security threat across the millions of ICTS transactions that remain in scope. Even with the interim rule's to-be-defined future licensing program, there is no practical guidance for companies to determine which of their millions of in-scope transactions may be prohibited, or perhaps licensable in the future. Without more clarity on scope and risk, companies may vary widely in their implementation, resulting in an inconsistent approach to supply chain security that will not achieve the purported goal of reducing or eliminating exposure to risky suppliers.

### **The Interim Rule Does Not Provide Adequate Due Process**

Due process requires that government provide advance notice of prohibited conduct so that the public may conform its behavior to comply. Because the interim rule remains so overly broad in terms of in-scope transactions and vague in terms of what constitutes undue or unacceptable risk, it does not provide adequate notice about what behavior is prohibited or problematic in the first place. As written, almost any ICTS transaction from one of the named foreign adversaries could be subject to the rule, if the Commerce Department determines that such transaction poses an undue or unacceptable risk, in its discretion. This lack of due process grants the government unprecedented authority to prohibit, or worse, unwind legitimate U.S. ICTS transactions without any real notice that those transactions were problematic in the first place. While a licensing process arguably could be beneficial, the interim rule only references a future process, without any clarity about how the licensing program will work or what types of transactions will require a license. This lack of sufficient notice places U.S. companies in an untenable position when navigating legitimate ICTS transactions in U.S. commerce that could be prohibited or unwound at some later date.

### **Conclusion**

IBM supports securing the global supply chain through precision regulation tailored to address defined national security threats. Unfortunately, the interim rule remains overly broad and does not identify the specific national security threats it intends to address. The result is a rule that does not advance the security of the supply chain in any meaningful way and that exposes U.S. companies to the economic uncertainty of having to avoid and/or unwind a broad scope of transactions. The excessive cost of this vague rule on the U.S. digital economy clearly

outweighs the elusive benefit. For this reason, we recommend that the Commerce Department suspend the interim rule and undertake a comprehensive review of the ICTS supply chain as part of the Administration's secure supply chain initiative to first identify supply chain risks and then develop pragmatic and implementable solutions to address them.

Sincerely,

A handwritten signature in black ink, appearing to read "Chris Padilla". The signature is fluid and cursive, with the first name "Chris" and last name "Padilla" clearly distinguishable.

Christopher A. Padilla  
Vice President  
Government and Regulatory Affairs

Attachments