Office of the Vice President
Government and Regulatory Affairs

600 14th Street, N.W. Suite 300
Washington, D.C. 20005

January 10, 2020

Mr. Henry Young
Senior Technology Policy Advisor
Office of the Secretary
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

ATTN: RIN 0605-AA51

Dear Mr. Young:

IBM hereby submits the following comments on the proposed rule: "Securing the Information and Communications Technology and Services Supply Chain" (Docket No. 191119-0084; RIN 0605-AA51), issued by the U.S. Department of Commerce on November 27, 2019 (the "Proposed Rule").

IBM shares the U.S. government's objective to improve security in the supply chain for information and communications technology products and services ("ICTS"). IBM depends on and takes great care to ensure a secure supply chain. We support thoughtful government efforts to protect the supply chain from threats presented by foreign adversaries.

This Proposed Rule, however, will not achieve this objective. It is massively overbroad and, if enacted in its current form, would harm the U.S. economy, fail to enhance U.S. national security, and violate principles of due process. The Proposed Rule should be revised, according to industry input, and re-issued as another proposed rule.

1. Massively Overbroad. The Proposed Rule authorizes the Department of Commerce to prohibit or unwind any "transaction" involving "ICTS" and a "foreign adversary" that poses either "undue risk" to ICT supply chains, critical infrastructure or "the digital economy of the United States," or "unacceptable risk" to U.S. national security. These and other terms are either undefined or defined so broadly that the Proposed Rule appears to subject hundreds of billions of dollars of legitimate U.S. commerce to vague and arbitrary government regulation.

2. Economic Harm. The Proposed Rule would create a costly contingent risk for <u>every</u> transaction subject to U.S. jurisdiction that involves ICTS. Many companies likely would respond by avoiding any market, product, technology or service that conceivably could trigger U.S. government review. The Proposed Rule therefore would lead to

substantial disengagement of U.S. businesses from global markets, reducing their competitiveness, threatening U.S. jobs, and hurting U.S. economic growth.

3. Failure to Enhance National Security. The Proposed Rule fails to establish criteria for or definitions of proscribed behavior that would allow companies to determine which transactions would be deemed to pose a national security threat. Thus, companies would be left to guess which transactions pose such a threat and may reach differing conclusions. The U.S. government will thus be put in the position of monitoring millions of transactions, something it will not have the resources to do. As a result, the Proposed Rule would fail to address in a systemic and consistent manner the threats posed by certain foreign suppliers and technologies.

4. Denial of Due Process. The Proposed Rule provides no guidance to companies as to what they may do and with whom they may do it. Moreover, it does not allow companies to seek the government's opinion about whether proposed transactions are prohibited or permitted. Instead, it appears to create a standard-less mechanism by which the government is authorized to block or unwind transactions, even years after the fact, effectively seizing private assets without compensation or due process.

For these reasons, the Commerce Department should go back to the drawing board to write an entirely different proposed regulation that clearly informs the public of what would be proscribed, provides a mechanism for advanced rulings, and creates market incentives for ICTS users to adopt approved supply chain standards. The public should then be given the opportunity to comment on that proposed rule.

The Proposed Rule Is Overbroad

The Proposed Rule authorizes the Department of Commerce to prohibit or unwind any "transaction" involving "ICTS" and a "foreign adversary" that poses either "undue risk" to ICT supply chains, critical infrastructure or "the digital economy of the United States," or "unacceptable risk" to U.S. national security.

The Proposed Rule fails to define what constitutes such an unacceptable risk, what standards the government will use to assess risk, or what specific behavior by private actors is proscribed. It does not specify any foreign adversaries or outline a process or standards by which the Secretary of Commerce will identify foreign adversaries. The Proposed Rule does not even acknowledge that the U.S. government has already sought to define the national security threats that should be guarded against.

For example, in August 2019, the U.S. Department of Homeland Security Cyber Infrastructure Security Agency ("CISA") identified what ICT hardware, software, and services present the greatest vulnerabilities in U.S. infrastructure. The Proposed Rule ignores this ongoing work, and instead would allow the Commerce Department essentially to use a "we-will-know-it-when-we-see-it" approach to determining what constitutes a national security threat and, having made such a determination, to impose any kind of restriction or prohibition it wants.

Further, the application of the Proposed Rule is so broad that it could capture under government control nearly every transaction in U.S. commerce. For example, as currently drafted, it authorizes the Commerce Department to prohibit or unwind any U.S. company's

"use" of ICTS from any foreign person, which is deemed to pose "an undue risk" to "the digital economy of the United States."

In practice, very little U.S. commercial activity today does not touch the digital economy. The Proposed Rule, therefore, would seemingly authorize the U.S. government to review or prevent almost any kind of transaction, including, for example:

- A U.S. bank employee using a laptop assembled in China (as virtually all are);
- A U.S. hospital attempting to use cloud-based software hosted in a data center;
- A U.S. telecommunications company installing new control equipment or antennae at a cell site; and
- A U.S. airline offering a mobile check-in application that contains even a single line of software code written by a foreign national.

The Proposed Rule is so broad that it does not just affect the use of ICTS in specified sensitive sectors such as critical infrastructure or hospitals. In its current form, the Proposed Rule would seem to cover the purchase or use of nearly *any* piece of IT equipment or *any* IT service, by *any* U.S. person. Nevertheless, the Proposed Rule offers no indication of how the Commerce Department would assign the resources or personnel necessary to conduct a fair and consistent review of all of those transactions.

Without parameters or process, market actors cannot be confident that the Commerce Department will establish a fair, transparent, or consistent regulatory process to implement the President's Executive Order of May 15. Instead, the Proposed Rule appears to give the Commerce Department nearly limitless jurisdiction and discretion to prohibit, even years after the fact, legal business transactions based on an unreviewable determination of an undefined security risk. This is a massively overbroad delegation of sweeping and arbitrary authority to unelected officials.

The Proposed Rule Threatens Economic Harm

The expansive and unprecedented scope of the Proposed Rule threatens the growth of the U.S. economy. As drafted, the Proposed Rule would allow the government to declare, unilaterally and after the fact, that legal commercial activity poses an undefined threat to national security and to prohibit it or demand that it be unwound. It could capture under government review hundreds of billions of dollars of legal services, research, and commercial activities.

By subjecting such a broad swath of U.S. commercial activity to review and potential restrictions or limitations, the Proposed Rule threatens significant harm to U.S. commercial and economic competitiveness. U.S. firms could be prevented from purchasing necessary equipment, forced to find more expensive or lower quality alternatives, or unable to develop certain products or services if they cannot use certain equipment. The Proposed Rule would open the door for foreign firms, unburdened by such overbroad and shortsighted rules, to displace the products and services of U.S. companies in global markets.

The Proposed Rule also inserts untenable uncertainty into a huge range of U.S. commercial transactions. By empowering the Commerce Department to negate any ICTS transaction for virtually any reason, the rule makes every business transaction with a foreign company conditional, impermanent, and potentially subject to unwinding many years later at the discretion of the Secretary of Commerce. Threatened with the possibility of having legitimate transactions retroactively prohibited, U.S. businesses will naturally avoid markets, products, suppliers, and transactions that pose even a remote chance of triggering Commerce Department review. This will lead to a broad disengagement of U.S. business from global markets and suppliers.

U.S. firms, facing a vacuum of guidance, will be left to guess what activity with whom could be restricted or prohibited. Particularly in the current political climate, companies may seek to eliminate all Chinese-sourced components from their supply chain and abstain from transactions with even the slightest nexus to China.

This outcome runs directly counter to the Administration's stated strategy of lowering market access barriers to China and promoting U.S. economic activity with China. In a recent speech, Vice President Pence said, "People sometimes ask whether the Trump Administration seeks to 'decouple" from China. The answer is a resounding, 'No.'"[1] The Proposed Rule contradicts this clear statement of U.S. policy. In addition, it likely will provoke reciprocal exclusion of U.S. ICTS suppliers from foreign markets, leading to further economic harm to the United States.

Finally, the Proposed Rule does not account for the reality of global supply chains, which are highly integrated. U.S. foundational ICTS infrastructure relies on components from many countries and parties that could be deemed "foreign adversaries." However, because the Proposed Rule does not provide specific criteria or processes for designating foreign adversaries, U.S. businesses must prepare for literally any foreign country or party to be so designated. The upshot will be a significant chilling effect on the growth of the U.S. ICTS sector and the U.S. economy.

The Proposed Rule Offers No Due Process

Due process requires that the government provide advance notice of prohibited conduct so that the public may conform its behavior to comply. The U.S. regulatory system has traditionally adhered to this principle by seeking to provide regulatory subjects with clear guidance on what conduct is prohibited. This tenet is never more critical than in the national security space.

Indeed, the Supreme Court has ruled that due process demands that laws and regulations provide advance notice of prohibited conduct so that the public has the opportunity to avoid violating the law. *See, e.g., FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 253–254 (2012). But this Proposed Rule is so vague and overbroad that it offers no due process. It articulates no standards by which to determine prohibited behavior or means to achieve compliance. It defines "transactions" to include any manner of business

[1] Vice President Mike Pence, Frederic V. Malek Memorial Lecture, Woodrow Wilson Center, October 24, 2019.

and "adopts a case-by-case, fact-specific approach to determine those transactions that . . . [are] prohibited or must be mitigated." It does not provide any mechanism for transactional pre-review or any standards by which to structure permissible transactions. It refuses even to name foreign adversaries, provide criteria for their future identification, or specify the national security threat at issue.

Instead, the Proposed Rule envisions that the government will take unprecedented actions – including retroactively – to prohibit legitimate transactions and confiscate property without due process of law. It does not even follow the guidance of the Executive Order, which suggests identifying particular countries or persons as foreign adversaries, identifying particular technologies or countries that will give rise to scrutiny, and establishing criteria by which market actors may be categorically included or excluded from the scope of application.

The Proposed Rule Will Not Enhance National Security and Should be Replaced with a New Proposed Regulation

The Proposed Rule would do little to strengthen the security of ICTS supply chains because it is so broad and so vague that there is no way for companies to comply. Without any definition of proscribed behavior, companies will be left to guess what constitutes a security threat and which ICTS suppliers should be avoided. Companies' choices may vary widely, leading to no consistent changes that would reduce or eliminate exposure to risky suppliers.

If companies are not provided sufficient guidance to comply, the U.S. government is left in the position of needing to monitor a seemingly vast range of transactions to identify and address risks. Yet the Proposed Rule does not establish a process or resource plan to do so. The Proposed Rule thus fails to address in a systemic and consistent manner the threats posed by certain foreign suppliers and technologies and will not enhance national security.

The Proposed Rule should be discarded and replaced with a new proposed regulation that fulfills the following criteria:

- It should clearly describe what type of transaction is prohibited, with which counterparties, and for what purpose;
- Its prohibitions should be risk-based and targeted at preventing a specific, articulated threat to U.S. national security;
- It should authorize parties to seek and receive advanced rulings on contemplated transactions; and
- It should eliminate any mechanism by which commercial competitors or aggrieved third parties could trigger Commerce Department review of another company's transactions.

The replacement rule *should also create market-based incentives* for companies to improve their own supply chain security practices. This can best be accomplished by exempting from regulation entities whose supply chain risk management processes satisfy standards contemplated by existing public-private supply chain security initiatives.

There are many such initiatives already underway. Among them are:

- The Department of Homeland Security Customs Trade Partnership Against Terrorism ("CTPAT"), which confers a number of benefits, such as fewer shipment inspections, on participants that adhere to specific cargo security requirements;
- The Department of Homeland Security ICT Supply Chain Risk Management Task Force, whose workstreams are informing the newly formed Federal Acquisition Security Council's policies and processes for agencies' acquisition of commercial IT products; and
- The Department of Defense ("DOD") Cybersecurity Maturity Model Certification program, which sets appropriate cybersecurity practices and processes criteria (articulated in NIST Special Publication 800-171) for doing business with the DOD – and is anticipated to result in a unified cyber standard for all of the U.S. government.

Companies that implement criteria pursuant to these U.S. government acquisition reform efforts will naturally migrate those supply chain security risk management practices to the commercial setting as well. The revised rule should therefore incentivize and encourage industry adherence to those existing standards (e.g. ISO 27000 series / ISO/IEC 27036 and ISO/IEC 20243) by creating a safe harbor for parties that implement these standards.

Conclusion

The Proposed Rule, in its current form, fails to protect supply chain security and harms the U.S. economy. Its reach, breadth, and vagueness are unprecedented. It provides no notice of what behavior is prohibited. It damages U.S. commerce by creating an ever-present threat of arbitrary executive action and is contrary to U.S. legal and regulatory principles. And because it is nearly impossible for companies to comply with this Proposed Rule, it will not enhance ICTS supply chain security. The harm it inflicts will dwarf any incidental benefit.

This Proposed Rule is deeply flawed and should be replaced with a new proposed regulation that clearly defines relevant terms and specific threats, provides companies the notice and predictability necessary to comply and continue to compete in the global economy, and puts in place market incentives for companies to implement already-established public-private supply chain standards.

Sincerely,

Christopher Padilla
Vice President
Government & Regulatory Affairs
IBM Corporation