Commerce Issues Proposed Rule Implementing "Supply Chain Executive Order"

December 3, 2019

Key Points

- On November 26, 2019, the U.S. Department of Commerce ("Commerce") issued a proposed rule to implement Executive Order 13873 of May 15, 2019, on "Securing the Information and Communications Technology and Services Supply Chain" ("Supply Chain EO"). The Supply Chain EO and proposed rule seek to create a broad framework to mitigate, prohibit and unwind information and communications technology and services (ICTS) transactions involving "foreign adversaries."
- The proposed rule does not designate specific governments or entities as "foreign adversaries." Nor does it identify any specific categories of transactions that are, or are not, subject to the regime. Rather, through the proposed rule, Commerce adopts a case-by-case, fact-specific approach to determine those transactions that meet the requirements set forth in the Supply Chain EO. While the proposed rule would establish certain procedural elements, it would not provide a pre-clearance or licensing mechanism to clear proposed transactions.
- If adopted as drafted, the proposed regulations could create significant uncertainty for companies operating in the ICTS sector. In particular, transactions with a nexus to China or Russia, which have informally been identified as "adversaries" in statements by U.S. government officials, would be at risk of intervention under this framework.
- Comments on the proposed rule are due by Friday December 27, 2019. Interested parties, including any company or organization involved in the ICTS sector, should carefully review the draft rules to assess their potential effect on any current or pending ICTS transactions and submit comments accordingly.

Background

On May 15, 2019, President Trump issued Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain or "Supply Chain EO" under the authority of the International Emergency Economic Powers Act (IEEPA). This statute allows the President to take certain actions to deal with any unusual and extraordinary foreign threat to the national security, foreign policy, or economy of the United States upon the President's declaration of a national

Contact Information

If you have any questions concerning this alert, please contact:

Christian C. Davis
Partner
chdavis@akingump.com
Washington, D.C.
+1 202.887.4529

Shiva Aminian
Partner
saminian@akingump.com
Los Angeles
+1 310.552.6476

Kevin J. Wolf
Partner
kwolf@akingump.com
Washington, D.C.
+1 202.887.4051

Tatman R. Savio
Registered Foreign Lawyer
tatman.savio@akingump.com
Hong Kong
+852 3694.3015

Clete R. Willems
Partner
cwillems@akingump.com
Washington, D.C.
+1 202.887.4125

Anne E. Borkovic
Partner
aborkovic@akingump.com
Washington, D.C.
+1 202.887.4432

Jaelyn Edwards Judelson
Counsel
jjudelson@akingump.com
Los Angeles
+1 310.552.6477

emergency with respect to that threat. In the Supply Chain EO, the President declared a national emergency with respect to the ability of "foreign adversaries" to create and exploit vulnerabilities in information and communications technology and services in order to commit malicious, cyber-enabled acts.

The primary impetus for this order is concern about the security of Chinese telecommunications equipment in the United States, and the need for regulation to address this concern, including by prohibiting certain transactions. The Trump Administration believes this is a gap in the national security legal framework since such activities are not captured under existing rules such as the U.S. foreign investment regimes administered by the Committee on Foreign Investment in the United States (CFIUS) or U.S. export controls, which govern exports, re-exports and transfers of certain commodities, software, technology and services.

Proposed Rule

On November 26, 2019, the U.S. Department of Commerce issued a proposed rule to implement the Supply Chain EO. Broadly, the proposed rule sets forth implementing regulations that would govern the procedures and high-level criteria applicable to the Department's evaluation of ICTS transactions falling within the scope of the Executive Order.

i. Key Definitions

The proposed rule does not provide additional guidance on key terms, but rather restates the following broad definitions set forth in the Supply Chain EO:

- "Information and communications technology or services" means "any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including through transmission, storage, or display."
- "Transaction" means "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service. Use of the term transaction in this part includes a class of transactions."
- "Foreign adversary" means "any foreign government or foreign non-government person determined by the Secretary of Commerce ("Secretary") to have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons for the purposes of Executive Order 13873."

ii. Scope

Rather than blanket prohibitions or restrictions on particular categories of ICTS transactions, the proposed rule would create a "case-by-case, fact specific" review process for specific transactions. Commerce states that this approach will allow it to properly "calibrate" the new authorities created by the Supply Chain EO without "unintentionally prohibiting" other ICTS transactions that present little or no risk to U.S. national security interests.

As currently drafted, the framework will apply to an ICTS transaction if:

- The transaction is conducted by any person subject to the jurisdiction of the United States or involves property subject to the jurisdiction of the United States;

Chris Chamberlain
Associate
cchamberlain@akingump.com
Washington, D.C.
+1 202.887.4308
John Callahan
Law Clerk
jcallahan@akingump.com
Washington, D.C.
+1 202.887.4025

- The transaction involves any property in which any foreign country or a national thereof has an interest (including through an interest in a contract for the provision of the technology or service),
- The transaction was initiated, is pending, or will be completed after May 15, 2019, regardless of when any contract applicable to the transaction was entered into, dated or signed, or when any license, permit, or authorization applicable to such transaction was granted. The proposed rule would also clarify that certain "ongoing activities," including but not limited to managed services, software updates or repairs, would constitute transactions that "will be completed" on or after May 15, 2019.;

Under the proposed framework, the Secretary could, in consultation with other agencies, require the mitigation, prohibition, or unwinding of any such transaction upon determining that:

- The transaction involves ICTS "designed, developed, manufactured, or supplied" by persons "owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary"; and
- The transaction poses:

  a. An undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;

  b. An undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or

  c. An unacceptable risk to the national security of the United States or the security and safety of United States persons. In the preamble of the proposed rule, Commerce states that "economic strength…is an essential element of our national security."

The proposed regulations provide further that in determining whether a transaction involves ICTS of a foreign adversary, Commerce will "consider a number of factors, including, but not limited to the laws and practices of the foreign adversary; equity interest, access rights, seats on a board of directors or other governing body, contractual arrangements, voting rights, and control over design plans, operations, hiring decisions, or business plan development."

iii. Process

Initiation and Evaluation – The proposed rule does not contemplate a voluntary or mandatory process for parties to notify and obtain pre-clearance for a transaction. Instead, it permits Commerce to commence an evaluation of an in-scope transaction (i.e., one that meets the criteria described above) in one of three ways:

- At the discretion of the Secretary.
- Upon request of a variety of other government agencies.
- Based upon information submitted to the Secretary by private parties that the Secretary "determines to be credible." The proposed rule would also create a web portal, through which private entities may provide such information.

The evaluation of the transaction would be informed by, among other sources, a threat assessment (i.e., focused on the foreign parties) produced by the Office of the Director of National Intelligence and a vulnerability assessment (i.e., focused on the vulnerability of the hardware, software and services) produced by the Department of Homeland Security. The proposed rule does not contemplate making these assessments public.

Notice and Response – Once a review has commenced, the proposed rule would require the Secretary to provide direct notice to involved parties that an evaluation is under way and that the Secretary has made a preliminary determination on whether the transaction presents national security concerns. Subject to extensions granted at the Secretary's discretion, the receiving party would then have 30 days to submit an opposition to that determination. Within 30 days of receiving information or opposition from the parties, the Secretary will issue a final determination, which would either clear or prohibit the transaction or require the parties to undertake specific mitigation measures for the transaction to proceed.

Emergency Action – In cases where "national security requires it," the proposed rule states that Commerce may "vary or dispense with any or all of the procedures" described above. The Secretary must only identify the basis for this decision in the final written determination.

Commentary and Analysis

i. Affected Entities and Sectors

In the proposed rule, Commerce identifies the following non-exhaustive list of the types of companies that it would expect to be directly affected by this regulation:

- Telecommunications and Information Technology Equipment and Service Providers
  - Telecommunications Service Providers:
  - Incumbent Local Exchange Carriers (LECs)
  - Interchange Carriers (IXCs)
  - Competitive Access Providers
  - Operator Service Providers (OSPs)
  - Local Resellers
  - Toll Resellers
  - Wired Telecommunications Carriers
  - Wireless Telecommunications Carrier (except Satellite)
  - Common Carrier Paging
  - Wireless Telephony
  - Satellite Telecommunications
  - All Other Telecommunications.
- Internet and Digital Service Providers:
  - Internet Service Providers (Broadband)

  - Internet Service Providers (Non-Broadband)
  - Cloud Providers
  - Data Center Service Providers
  - Managed Security Service Providers
  - Internet Application Operators/Developers
  - Software Providers (platform as a service, software as a service, etc.).
- Vendors and Equipment Manufacturers
  - Vendors of Infrastructure Development or "Network Buildout"
  - Telephone Apparatus Manufacturing
  - Radio and Television Broadcasting and Wireless Communications Equipment
  - Information Technology Equipment Manufacturers
  - Connected Device Manufacturers (e.g., connected video cameras, health monitoring devices)
  - Other Communications Equipment Manufacturing.

As Commerce notes, "[a] majority of entities today…utilize some manner of ICTS, therefore it is extremely difficult to [determine the full impact of the proposed rule]." In this context, the types of companies affected by this rule could stretch well beyond those identified above.

ii. CFIUS Authority But Broader and Without the Process

The proposed framework is similar to the CFIUS regime but ultimately much broader in scope, as the primary limitations on the scope of review are merely that a "transaction" (broadly defined) involves a "foreign adversary" and ICTS. In addition, the proposed regulations would not permit Commerce to issue "advisory opinion[s]" or "declaratory ruling[s]" with respect to any proposed transaction, which differs sharply from the CFIUS voluntary notification process. In effect, the proposed regulations would provide no mechanism for clearing a potentially prohibited transaction prior to its consummation (the execution of which could trigger civil penalties under the proposed rule). As noted above, the draft regulations also would not categorically include or exclude any types of ICTS transactions (though this is a topic on which Commerce has requested specific comments from industry).

Opportunity to Comment

Topics of Interest – Commerce invites general comments on the proposed rule and, in particular, requests comments on the following:

1. With respect to the proposed "case-by-case" approach:

- Should Commerce consider categorical exclusions?
- Are there classes of persons whose use of ICTS can never violate the EO? If so, please provide a detailed explanation of why the commenter believes a particular transaction can never meet the requirements of the EO.

2. With respect to mitigation:

- Are there transactions involving types or classes of ICTS where the acquisition or use in the United States or by U.S. parties would fall within the terms of the EO's prohibited transactions because the transaction could present an undue or unacceptable risk, but that risk could be reliably and adequately mitigated to prevent the undue or unacceptable risk?
- If the commenter believes the risks of a prohibited transaction can be mitigated, what form could such mitigation measures take?

3. With respect to mitigation enforcement:

- If mitigation measures are adopted for a transaction otherwise prohibited by the EO, how should the Secretary ensure that parties to such transaction consistently execute and comply with the agreed-upon mitigation measures that make an otherwise prohibited transaction permissible?
- How best could the Secretary be made aware of changes in factual circumstances, including technology developments, that could render mitigation measures obsolete, no longer effective, or newly applicable?

4. With respect to the definition of "transaction":

- Section 1(a) of the EO and the definition of "transaction" that the proposed rule would implement refer to "acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service." How are these terms, in particular "dealing in" and "use of," best interpreted?

5. With respect to recordkeeping:

- The Secretary expects persons engaged in transactions will maintain records of those transactions in the ordinary course of business. Should the Department require additional recordkeeping requirements for information related to transactions?

Ex Parte Comments – According to the Federal Register notice, any "non-public oral communication" to Commerce officials regarding the "substance of the proposed rule" will be considered an ex parte presentation, and a summary of the communication will be placed in the public record. The notice further provides that parties may, within two business days after such communication, submit a written summary of the communication, which Commerce may (or request that the submitting party) supplement to include any "important information [that] was omitted or characterized incorrectly." These written submissions will also become part of the public record.

Interested parties have until Friday, December 27, 2019, to submit comments for consideration via the Federal eRulemaking Portal, emailing ICTsupplychain@doc.gov, or by mail or hand delivery to Commerce headquarters in Washington, D.C.

Conclusion

The proposed rule could create potential uncertainty with respect to any transaction involving the ICTS sector and bestow broad authority on Commerce. Companies will have limited information to identify potentially relevant national security concerns or to know when they are triggered, and the proposed rule does not provide a mechanism for clearing transactions prior to proceeding. Given the broad implications, we

recommend that affected parties carefully consider the implications on their business and assess whether to submit public comments.

akingump.com