COMMERCE PROPOSES PROCESS TO EVALUATE TRANSACTIONS INVOLVING INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES FOR NATIONAL SECURITY CONCERNS

Date: 3 December 2019

U.S. International Trade Alert

By: Steven F. Hill, Jeffrey Orenstein, Erica L. Bakies, Stacy J. Ettinger

On November 27, 2019, the Department of Commerce ("Commerce") issued a proposed rule implementing Executive Order ("EO") 13873, "Securing the Information and Communications Technology and Services Supply Chain," issued on May 15, 2019. The proposed rule sets forth the procedures that Commerce intends to use to identify, review, and address transactions involving information and communications technology and services ("ICTS") that pose an undue risk to critical infrastructure or the digital economy in the United States, or unacceptable risk to U.S. national security or U.S. persons. Here are the key takeaways:

- ICTS is defined as "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."
- The proposed rule would apply to "any acquisition, importation, transfer, installation, dealing in, or use of any" ICTS ("transaction") that (1) is subject to U.S. jurisdiction or involves property subject to U.S. jurisdiction, (2) involves property in which a foreign country or national thereof has an interest, and (3) was initiated, is pending, or will be completed after May 15, 2019. Transactions include ongoing activities, such as managed services, software updates, or repairs, even if the initial transaction was initiated, pending, or completed **before** May 15, 2019.
- In the event that a transaction presents an undue risk to critical infrastructure or the digital economy in the United States or an unacceptable risk to U.S. national security or U.S. persons, Commerce could require the transaction parties to implement mitigation measures, or prohibit the transaction in its entirety.
- Private parties will be able to notify Commerce of transactions that poses an undue risk to critical infrastructure or the digital economy in the United States or an unacceptable risk to U.S. national security or U.S. persons.
- The proposed rule does **not** include a process by which parties to transactions that potentially present national security concerns can seek review from Commerce.
- Comments on the proposed rule are due no later than December 27, 2019.

THE EVALUATION PROCESS

The proposed rule sets forth the process by which Commerce will evaluate transactions subject to the rule. Evaluations can be commenced in one of three ways:

1. At Commerce's discretion;
2. Upon the request of another government department, agency, governmental body, or the Federal Acquisition Security Council; or
3. Based on information provided by private parties.

Each evaluation will be based on the particular facts and circumstances of the transaction; however, in the future, Commerce may designate classes of transactions for categorical inclusion or exclusion. For each evaluation, Commerce will consult with other agencies, including the Department of the Treasury, the Department of State, the Department of Defense, the Attorney General, the Department of Homeland Security, the U.S. Trade Representative, the Director of National Intelligence, the General Services Administration, the Federal Communications Commission, and others, as appropriate. An evaluation will consider:

4. Whether the transaction is subject to U.S. jurisdiction;
5. Whether the transaction involves property in which a foreign country or national has an interest;
6. Whether the transaction was initiated, is pending, or will be completed after May 15, 2019 (including follow-on services);
7. Whether 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 [1]; and
8. Whether the transaction:
    - Poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of ICTS in the United States;
    - Poses an undue risk of catastrophic effects on the security or resiliency of U.S. critical infrastructure or the digital economy of the United States; or
    - Otherwise poses an unacceptable risk to the national security of the United States or the security and safety of U.S. persons.

If a transaction comes under review, Commerce will notify the relevant parties and will also provide notification of the preliminary determination. [2] The transaction parties will then have 30 days to submit written opposition and relevant information, which could include proposed mitigation measures. After receipt of the written opposition and other relevant information, Commerce will issue a final decision within 30 days. The final decision will inform parties that Commerce either has prohibited the transaction, has not prohibited the transaction, or is requiring mitigation measures. [3] Commerce will publish summaries of its reviews on its public website and through the *Federal Register*.

The proposed rule also provides that Commerce may alter or dispense with any or all of the foregoing procedures in the event that following the procedures would likely result in public harm or national security interests require it.

Violations of the proposed rule or any mitigation measure or material condition would carry a civil penalty of up to $302,584, as adjusted for inflation, or an amount that is twice the amount of the transaction that is the basis for

the violation with respect to which the penalty is imposed. The precise amount will depend on the nature of the violation.

INITIAL REACTIONS

Companies likely to be impacted by this rule include:

9. Telecommunications and information technology equipment and service providers, such as wired and wireless telecommunications carriers, wireless telephony, satellite telecommunications, and all other telecommunications;
10. Internet and digital service providers, such as broadband and non-broadband internet service providers, cloud providers, data center service providers, managed security service providers, internet application operators/developments, and software providers; and
11. Vendors and equipment manufacturing, such as 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, and other communications equipment manufacturers.

As drafted, the evaluation process does not allow parties to seek prospective review of a potential transaction to determine if it presents an undue risk to critical infrastructure or the digital economy in the United States or an unacceptable risk to U.S. national security or U.S. persons. Commerce specifically stated that it "will not issue an advisory opinion or a declaratory ruling with respect to a particular transaction." As such, companies likely to be impacted by this rule should continue to monitor the implementation of this rule to understand the types of transactions that Commerce believes present an undue risk to critical infrastructure or the digital economy in the United States or an unacceptable risk to U.S. national security or U.S. persons.

Finally, the proposed rule allows the public to bring to Commerce's attention certain transactions that could pose an undue risk to critical infrastructure or the digital economy in the United States or an unacceptable risk to U.S. national security or U.S. persons. This presents an initial concern that companies could submit information on the transactions of their competitors in an effort to gain an edge in the market.

NEXT STEPS

Comments on the proposed rule are due on December 27, 2019. Commerce is seeking comments on the entire proposed rule. However, Commerce is particularly interested in hearing from the industry regarding (1) whether there are any categorical exclusions that Commerce should consider, (2) options for various mitigation measures, and (3) ensuring compliance with mitigation measures. K&L Gates is well positioned to assist with the preparation of such comments.

Continue to follow K&L Gates as we track the implementation of EO 13873 and Commerce's proposed rule. Contact any of the authors for additional information on this or any other related topic.

NOTES:

[1] Whether a person is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary includes considerations such as 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.
[2] At that point, parties will be required to take steps to retain any and all records relating to the transaction.
[3] In the event that there are any material changes to the transaction, Commerce may commence a new evaluation and make a new determination.

KEY CONTACTS

STEVEN F. HILL
PARTNER

WASHINGTON DC
+1.202.778.9384
STEVEN.HILL@KLGATES.COM

JEFFREY ORENSTEIN
PARTNER

WASHINGTON DC
+1.202.778.9465
JEFFREY.ORENSTEIN@KLGATES.COM

