Milbank

Global Risk & National Security Group

Client Alert

President Trump Declares National Emergency to Counter Threats to U.S. Technology Supply Chain Posed by Foreign Adversaries

May 17, 2019

Contact

Dara A. Panahy, Partner
+1-202-835-7521
dpanahy@milbank.com

Bijan Ganji, Associate
+1-202-835-7543
bganji@milbank.com

Lafayette Greenfield, Associate
+1-202-835-7564
lgreenfield@milbank.com

Sean Heiden, Associate
+1-202-835-7536
sheiden@milbank.com

On May 15, 2019, President Donald Trump issued an Executive Order on Securing the Information and Communications Technology and Services Supply Chain (the "Executive Order"). The Executive Order seeks to protect U.S. communications infrastructure against threats of infiltration and sabotage by foreign actors. Based on other recent and contemporaneous actions by the Trump Administration, as discussed further below, the Executive Order is considered to have been motivated, at least in part, by U.S. government concerns relating to Huawei Technologies Co. Ltd. ("Huawei"), the Chinese telecommunications company regarded by the Administration to be engaged in "activities that are contrary to U.S. national security [and] foreign policy interest[s]."

Specifically, the Executive Order prohibits persons subject to U.S. jurisdiction from acquiring, importing, transferring, installing, dealing in or using any information and communications technology or service that the Secretary of Commerce (the "Secretary"), in consultation with the Secretary of the Treasury, the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the United States Trade Representative, the Director of National Intelligence, the Administrator of General Services, the Chairman of the Federal Communications Commission, and, where appropriate, the heads of other executive departments and agencies, has determined:

> (i) involves information and communications technology or services designed, developed, manufactured, or supplied, by entities owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and
>
> (ii) poses (A) an undue risk of sabotage to or subversion 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 U.S. persons.

The Executive Order empowers the Secretary to halt already initiated or pending transactions, but provides that certain otherwise prohibited transactions may be allowed if effective, Secretary-approved mitigation measures can be negotiated and implemented to minimize the perceived risks to U.S. national security.

The Secretary is required under the Executive Order to publish, within 150 days of the date of the Executive Order, implementing regulations in consultation with other Cabinet Secretaries and the heads of Executive Branch agencies. Such implementing regulations are expected to include identifications, processes or clarifications with respect to:

- Countries or persons that are "foreign adversaries";
- Entities owned by, controlled by or subject to the jurisdiction or direction of "foreign adversaries";
- Particular information and communications technologies or services that warrant heightened scrutiny;
- Criteria for the categorical inclusion or exclusion of certain technologies or market participants from the prohibitions of the Executive Order; and
- Review and/or licensing of, and/or mitigation of national security risks inherent to, pending or contemplated transactions.

Also on May 15, 2019, the U.S. Department of Commerce (the "Commerce Department") designated Huawei and 70 of its affiliates on the Entity List, which is maintained by the Commerce Department under the Export Administration Regulations. Parties identified on the Entity List are prohibited from receiving exports or transfers of U.S. export-controlled items unless the exporting party obtains, in advance, an export license from the Commerce Department's Bureau of Industry and Security.

*****

This Client Alert provides a summary of certain key elements of the Executive Order and is not comprehensive as to the full scope of the Executive Order or any implementing regulations, or other elements of the legal framework, that may relate to or follow from the Executive Order.

Washington, D.C. | 1850 K Street, NW, Suite 1100, Washington, D.C. 20006

Dara A. Panahy dpanahy@milbank.com +1-202-835-7521

Global Risk & National Security Practice Group

Please feel free to discuss any aspects of this Client Alert with your regular Milbank contacts or any member of our Global Risk & National Security Practice Group.

This Client Alert is a source of general information for clients and friends of Milbank LLP. Its content should not be construed as legal advice, and readers should not act upon the information in this Client Alert without consulting counsel.