STEPTOE OUTSIDE COUNSEL

Demystifying the ICTS Supply Chain Rule

In January 2021, the Commerce Department published an interim final rule entitled "Securing the Information and Communications Technology and Services Supply Chain,"[1] which implements a Trump administration executive order[2] directing the Department to create a review process for certain transactions involving information and communications technology or services ("ICTS") linked to "foreign adversaries".

What's the goal of this new rule?

The rule authorizes Commerce to prohibit or regulate transactions involving ICTS, when linked to a foreign adversary, that pose an "undue or unacceptable risk" to US national security.

Are my activities covered?

The easiest way to know may be to assess whether a transaction involves a so-called foreign adversary. Currently, the rule lists six jurisdictions as foreign adversaries: China (including Hong Kong), Russia, Cuba, Iran, North Korea, and the Maduro regime in Venezuela. However, the rule can potentially apply to products or services provided from third countries if they were designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary. The rule broadly defines "subject to the jurisdiction or direction of a foreign adversary" to include acting "under the direction or control of a foreign adversary or of a person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary."

Another way to tell if a transaction is covered is by considering whether it involves any of the six categories of ICTS that are subject to the rule. These categories, which are described in detail in the rule, include: critical infrastructure, networks and satellites, sensitive personal data, monitoring and home networking devices (including drones), Internet/telecommunications software, and emerging technology.

What if my activities are covered?

Notably, the rule doesn't impose a general prohibition on the importation or use of ICTS from foreign adversaries, but instead enables Commerce to review such transactions and prohibit specific transactions or order modifications or mitigations to address US national security concerns. The rule provides a process for rendering decisions regarding ICTS, including an opportunity for parties to the activity in question to respond to Commerce's findings.

The rule sets forth ten broad criteria to evaluate the risk of an ICTS transaction in light of US national security concerns. For example, the Secretary may consider the technical capabilities, market share, vulnerability, potential for mitigation, and the nature and degree of the foreign adversary's involvement, among other factors. In late March 2021, Commerce issued an advanced notice of proposed rulemaking regarding the creation of a licensing process for parties to seek "pre-approval" for a given transaction.[3] That rulemaking process is ongoing.

How has the rule been enforced?

It is still early in the rule's implementation and much remains to be seen. However, Commerce has indicated it plans to use the rule fairly aggressively, particularly with respect to China. At the time of this writing, Commerce has announced the issuance of administrative subpoenas to multiple Chinese companies that provide ICTS to the US, suggesting it is actively exercising its new authorities.[4]

How should I prepare?

You can start by identifying whether any of your company's transactions involve (1) ICTS and (2) a foreign adversary as those terms are defined under the rule. If any transactions are subject to the rule, a prudent next step would be to consider whether the transactions seem likely to raise national security concerns based on the ten criteria in the rule. If any transactions seem as though they could be of interest to Commerce it may be worth exploring ways to mitigate any potential risks, seeking advice from counsel, potentially engaging with Commerce proactively, and/or seeking pre-approval once the process is implemented. ■

About the authors:
Meredith Rathbone is a Partner (Mrathbone@steptoe.com) and Evan Abrams is an Associate (eabrams@steptoe.com) in Steptoe's Washington, DC office.

[1] 15 C.F.R. Part 7.
[2] Executive order 13873, Securing the Information and Communications Technology and Services Supply Chain (15 May 2019), https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.
[3] Securing the Information and Communications Technology and Services Supply Chain: Licensing Procedures, 86 Fed. Reg. 16,312 (29 March 2021), https://www.govinfo.gov/content/pkg/FR-2021-03-29/pdf/2021-06529.pdf.
[4] US Dep't of Commerce: U.S. Secretary of Commerce Gina Raimondo Statement on Actions Taken Under ICTS Supply Chain Executive Order (17 March 2021): https://www.commerce.gov/news/press-releases/2021/03/us-secretary-commerce-gina-raimondo-statement-actions-taken-under-icts; US Dep't of Commerce: U.S. Department of Commerce Statement on Actions Taken Under ICTS Supply Chain Executive Order (13 April 2021), https://www.commerce.gov/news/press-releases/2021/04/us-department-commerce-statement-actions-taken-under-icts-supply-chain.

Reprinted with permission from the May 2021 issue of Export Compliance Manager
www.exportcompliancemanager.com