

On January 19, 2021, regulations were [published](#) in the US *Federal Register* implementing Executive Order 13873 of May 15, 2019, “Securing the Information and Communications Technology and Services Supply Chain” ([84 FR 22689](#)).

These regulations give the US Department of Commerce (Commerce) regulatory authority over certain transactions involving information and communications technology and services (ICTS) (e.g., hardware, software or services used in specific IT or communications applications), where those ICTS are “designed, developed, manufactured, or supplied” by businesses subject to the jurisdiction of “foreign adversaries,” which includes the People’s Republic of China (China). Under the new rule, Commerce can address and mitigate national security concerns associated with these transactions. Our publication includes a brief summary of the types of commercial transactions captured by the regulations and offers considerations for how businesses may address risks in their supply chains or customer bases. For questions and further details, please reach out to any member of our team listed at the end of this publication.

What Types of Products and Services Fall Within ICTS?

ICTS encompasses any product or service (including hardware, software and cloud-computing services) that is “primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means,” including by “transmission, storage, or display.” Such products and services include ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download.

How Will Commerce Review “Covered ICTS Transactions”?

Commerce has the authority to review any acquisition, importation, transfer, installation, dealing in or use of any ICTS (an “ICTS Transaction”) to determine if it is a “Covered ICTS Transaction,” and if the ICTS has been designed, developed, manufactured or supplied by persons owned by, controlled by or subject to the jurisdiction or direction of foreign adversaries – currently designated as China (which includes the Hong Kong Special Administrative Region (SAR)), Cuba, Iran, North Korea, Russia and the Maduro Regime of Venezuela. For Covered ICTS Transactions that fall within its authority, Commerce can prohibit the transaction or propose mitigation measures to address any undue or unacceptable risks.

What Transactions Are “Covered ICTS Transactions”?

The regulations specify that ICTS Transactions involving certain technologies, hardware or software will be considered to be Covered ICTS Transactions. With limited exceptions, a Covered ICTS Transaction means any ICTS Transaction that:

1. Is conducted by any person subject to US jurisdiction or involves property subject to US jurisdiction
2. 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)
3. Involves a transaction that was initiated, pending or completed on or after January 19, 2021
4. Involves one of the six categories of ICTS end uses ([see here for a summary of those categories](#))

What Constitutes the Commerce Review Process?

Upon learning of an ICTS Transaction (from any number of sources), Commerce will immediately assess (1) whether the transaction is a Covered ICTS Transaction; and (2) whether the ICTS 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.” Commerce will then either accept and commence an initial review of the transaction; request additional information; or end the inquiry. If Commerce undertakes an initial review, it will coordinate an interagency process and may request information from the parties. This process will result in an “initial determination” by Commerce to allow the transaction to proceed or, alternatively, to prohibit the ICTS Transaction or to propose mitigation measures. If the latter, parties have 30 days to respond to the initial determination. Upon consideration of the parties’ submissions, Commerce will issue a final determination in coordination with other agencies (and the President, if necessary) that will either (1) prohibit the transaction; (2) not prohibit the transaction; or (3) permit the transaction subject to the adoption of mitigation measures determined by Commerce. This process, from start to final determination, occurs within 180 days, unless extended by Commerce.

Is There a Forthcoming Licensing Process?

Commerce is expected to issue additional regulations that will implement a licensing regime on or around March 22, 2021, and implement that rule by May 19, 2021. The procedures will establish criteria for any parties to a proposed, pending or ongoing ICTS Transaction to seek a license for that ICTS Transaction. According to Commerce, “[l]icense application reviews will be conducted on a fixed timeline, not to exceed 120 days from accepting a license application.”

When Do the Regulations Go Into Effect and Will They Apply Retroactively?

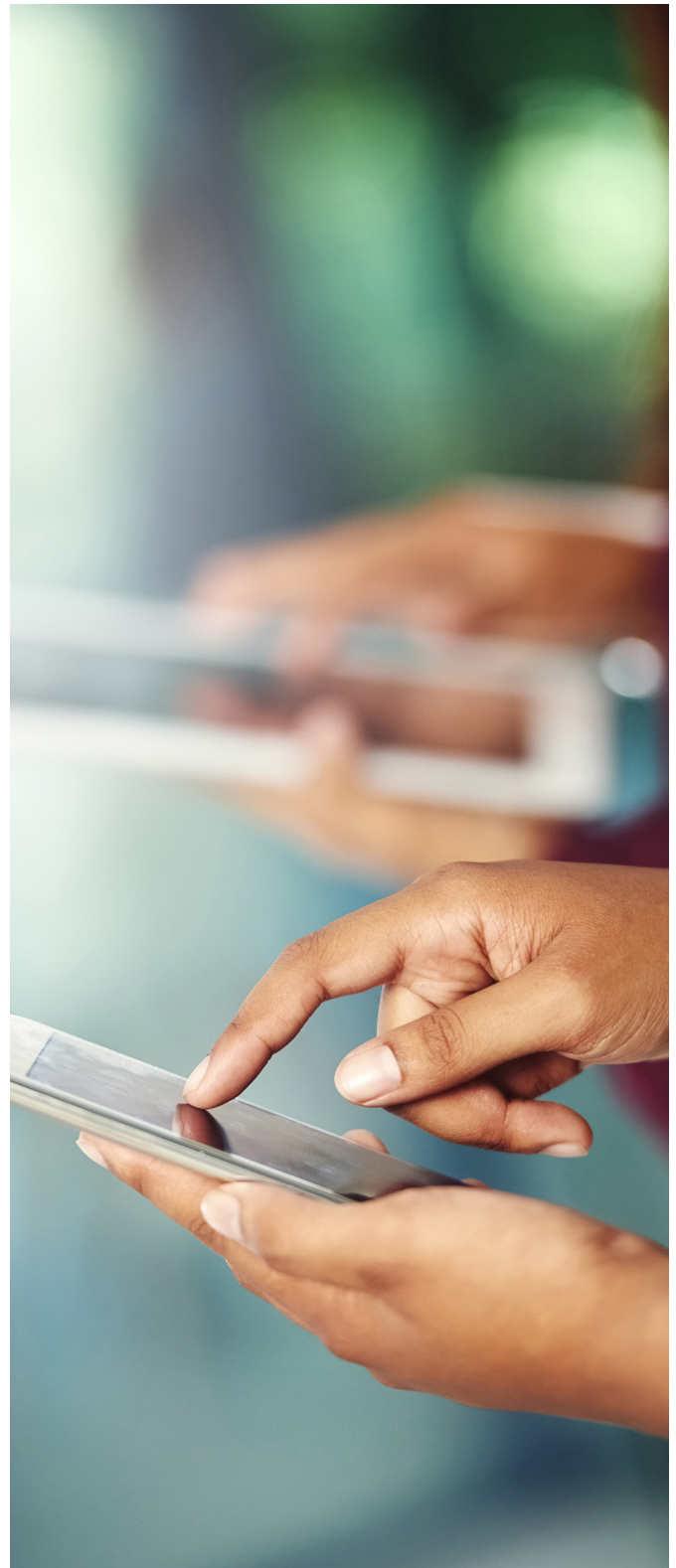
The regulations were issued as an Interim Final Rule and will take effect on March 22, 2021. In the meantime, Commerce is accepting further public comment before issuing a final rule. However, the just issued regulations will apply to any ICTS Transaction that was “initiated, pending, or completed” on or after January 19, 2021.

Considerations for Navigating the New Rule

These regulations will extend authority into the supply chains of any company doing business in the US in the six categories of ICTS end uses ([see our summary reference chart of these categories here](#)) within the scope of Covered ICTS Transactions. Importantly, the regulations do not require that a transaction directly involve a business from a “foreign adversary.” Instead, Commerce will assess whether that transaction “involves ICTS designed, developed, manufactured, or supplied” by persons subject to the jurisdiction of a foreign adversary.

For example, a transaction between a Japanese component supplier and a US data center business could be reviewed by Commerce upon a finding that the Japanese company was providing ICTS products originally designed or supplied by Chinese sources.

US businesses with operations in one of the six defined subject areas should analyze their supply chains, if they have not started already, to assess the level of regulatory risks and burdens created by the new regulations. Equally as important, global suppliers in China should analyze their US customer base and downstream US markets to determine the level of exposure that their businesses have under the new regulations. Depending on the types of customers and downstream industries served, global suppliers may want to evaluate proactive measures in advance of the effective date of the new authorities.



Contacts

Trade Practitioners [George Grammas](#), [Peter Alfano](#), and [Paul Besozzi](#) (partner, Communications Practice) are available to answer questions or offer assistance.

International Trade Team

Please contact one of the trade practitioners listed or you can reach our team collectively at internationaltradecompliance@squirepb.com.

US		
George Grammas Partner, Washington DC/London Co-Chair, International Trade – Trade Compliance and National Security T +1 202 626 6234 T +44 20 7655 1301 E george.grammas@squirepb.com	Daniel E. Waltz Partner, Washington DC T +1 202 457 5651 E daniel.waltz@squirepb.com	Karen R. Harbaugh Partner, Washington DC T +1 202 457 6485 E karen.harbaugh@squirepb.com
EU		
Robert MacLean Partner, Brussels T +32 2 627 7619 E robert.maclean@squirepb.com	José María Viñals Partner, Madrid/Brussels T +34 91 426 4840 T +32 2 627 1111 E josemaria.vinals@squirepb.com	Wojciech Maciejewski Associate, Brussels T +32 2 627 7612 E wojciech.maciejewski@squirepb.com
UK		
Matthew Kirk International Affairs Advisor, London T +44 20 7655 1389 E matthew.kirk@squirepb.com		

International Trade Practice co-leaders: Frank Samolis (partner, Washington DC) and George Grammas

About Us

Our export controls and sanctions lawyers have the ability to provide advice on the shifting regulatory framework on both sides of the Atlantic. We have extensive experience in advising and representing a wide range of companies and financial institutions in Europe, the US and other jurisdictions on export control and sanctions from a multijurisdictional perspective. Our team is part of our overall International Trade Practice, providing a “one-stop shop” solution to global trade compliance through rapid, professional and tailored advice and compliance tools to fit your business needs and processes.

ITAR Handbook

Organizations engaged in the trade of items specially designed for military or space applications are encouraged to download our complimentary ITAR Practitioner’s Handbook, which covers the International Traffic in Arms Regulations (ITAR) and the US Department of Commerce “600 Series.”