Regulatory Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Commerce Proposes ICTS Changes for Connected Software Applications

December 01, 2021

Key Points

- On November 26, 2021, the U.S. Department of Commerce issued a notice of proposed rulemaking related to "connected software applications" ("apps") that aims to expressly incorporate transactions involving apps into the scope of the ICTS Supply Chain regulations.
- More specifically, the Proposed Rule would update the ICTS Supply Chain regulations to explicitly include "connected software applications" in the definition of "information and communications technology or services" and affirm that transactions involving apps fall within the scope of covered ICTS transactions.
- The Proposed Rule also sets forth potential indicators of risk for the Secretary of Commerce to consider when assessing whether an ICTS Transaction involving connected software applications poses an undue or unacceptable risk under the ICTS Supply Chain regulations.
- Comments on the Proposed Rule are due on December 27, 2021.

Background

On November 26, 2021, the U.S. Department of Commerce ("Commerce") issued a proposed rule, "Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications" (the "Proposed Rule"), to amend the Information and Communications Technology and Services (ICTS) Supply Chain regulations (15 C.F.R. Part 7) that became effective on March 22, 2021. Those regulations implement Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain ("ICTS Supply Chain EO") issued by former President Trump on May 15, 2019 to address the national emergency posed by the ability of "foreign adversaries" to create and exploit vulnerabilities in the ICTS supply chain.[1] Generally speaking, the ICTS Supply Chain regulations provide a broad framework for the Secretary of Commerce to identify, mitigate, prohibit or unwind covered "ICTS Transactions"[2] involving "foreign adversaries"[3] that pose an undue or unacceptable risk to U.S. national security.

Contact Information

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

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

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

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

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

Katherine P. Padgett
Counsel
kpadgett@akingump.com
Washington, D.C.
+1 202.887.4079

William A. McClure
Associate
wmcclure@akingump.com
Washington, D.C.
+1 202.887.4512

Thor Petersen
Associate
tpetersen@akingump.com
Washington, D.C.
+1 202.887.4307

In parallel and relying on the national emergency declared in the ICTS Supply Chain EO, in the last six months of his administration, President Trump issued three Executive Orders targeting specific Chinese apps, including TikTok, WeChat and eight other Chinese software applications (EOs 13942, 13943 and 13971). Following various legal challenges, and a change in administration, President Biden issued Executive Order 14034: "Protecting American's Sensitive Personal Data from Foreign Adversaries" ("EO 14034") on June 9, 2021. In addition to revoking the three Trump-era "app ban" EOs, EO 14034 directed the Secretary of Commerce to undertake any further consideration of the risks posed by apps under the ICTS Supply Chain regulations and identified several app-specific risk factors (discussed further in the next section below) for the Secretary to evaluate as part of any review.[4]

Proposed Rule

The Proposed Rule makes largely technical changes to the ICTS Supply Chain regulations based on EO 14034. The primary impact of the Proposed Rule is to add express references to "connected software applications" in the ICTS Supply Chain regulations where relevant. Notably, the Proposed Rule states that these changes do "not increase the scope of applicability of the existing regulations," and are intended to make clearer that transactions involving "connected software applications" are within the scope of the ICTS Supply Chain regulations.

Specifically, in addition to adding "connected software applications" to the definitions and purpose sections of the regulations, the Proposed Rule confirms that certain transactions involving "connected software applications" fall within the category of "Covered ICTS Transactions" involving software "designed primarily for connecting with and communicating via the internet that is used by greater than one million U.S. persons."

As noted above, the Proposed Rule also incorporates the app-specific risk factors set forth in EO 14034 that should be considered in evaluating whether an ICTS Transaction involving connected software applications poses an undue or unacceptable risk. Those "potential indicators of risk" include:

- Ownership, control or management by persons that support a foreign adversary's military, intelligence or proliferation activities.
- Use of the connected software application to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data.
- Ownership, control or management of connected software applications by persons subject to coercion or cooption by a foreign adversary.
- Ownership, control or management of connected software applications by persons involved in malicious cyber activities.
- A lack of thorough and reliable third-party auditing of connected software applications.
- The scope and sensitivity of the data collected.
- The number and sensitivity of the users of the connected software application.
- The extent to which identified risks have been or can be addressed by independently verifiable measures.

Comment Period

The Proposed Rule calls for comments on a number of topics, including:

- The definition of "connected software applications" and whether it is properly scoped and incorporates the correct industry terminology.
- Whether there are other app-specific factors that should be added to the "connected software applications" risk criteria and whether those factors should be applied more generally to all ICTS Transaction reviews.
- The scope and meaning of specific terms as used in those app-specific potential indicators of risk including "ownership, control or management," "reliable third-party," "independently verifiable measures" and "third-party auditing," among others.

Comments to the Proposed Rule must be received on or before December 27, 2021, via the Federal eRulemaking Portal or by emailing ICTsupplychain@doc.gov.

Next Steps

The Proposed Rule will not become effective until Commerce reviews the comments received and issues a final rule, though as noted above, the Proposed Rule does not technically expand the scope of covered ICTS Transactions that are subject to Commerce review under the ICTS Supply Chain regulations. With that in mind, industry has the opportunity prior to December 27, 2021 to shape the treatment of apps under the ICTS Supply Chain regulations through public comments.

Meanwhile, more broadly, Commerce is still expected to provide greater clarity regarding the ICTS regime, including by issuing a proposed rule regarding an ICTS licensing regime, and identifying which office within Commerce will administer the ICTS regime. Still, because the ICTS Supply Chain regulations remain in effect, we may see parallel enforcement-related actions from Commerce, including requests for information, issuances of additional subpoenas, or perhaps even enforcement actions involving specific, identified ICTS Transactions.

[1] For more information on the ICTS Supply Chain EO and regulations, please see our prior alerts on this topic (May 2019, December 2019 and February 2021).

[2] The ICTS Supply Chain implementing regulations define "ICTS Transaction" to mean "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download."

[3] The ICTS Supply Chain regulations designate China (including Hong Kong), Cuba, Iran, North Korea, Russia and Venezuela's Maduro regime as "foreign adversaries."

[4] For more information on the EO 14034, please see our prior alert on this topic.

akingump.com