Preparing For Enforcement Of IT Supply Chain Security Rule

By **Tyler Grove and John Hannon** (February 8, 2023)

Tyler Grove

John Hannon

The U.S. Department of Commerce has begun to employ a novel and powerful regulatory tool to address national security risks in the information and communications technology and services, or ICTS, supply chain.

Following a rulemaking in the final days of the Trump administration, Commerce now has authority to review and potentially unwind certain transactions with entities connected to so-called foreign adversaries, including China and Russia.

Commerce's powers under the ICTS rule are similar to those of the Committee on Foreign Investment in the United States, although the ICTS rule potentially reaches a broader range of entities and activities than does the CFIUS regime.

In its most recent budget, Commerce requested approximately $36 million dollars to hire 114 positions dedicated to ICTS administration and enforcement. In recent weeks, there have also been public reports emerging of ICTS subpoenas being issued to various companies.

With growing indications that Commerce may imminently begin robust ICTS enforcement, companies potentially affected by the ICTS rule should begin to proactively prepare to respond using guidance and mitigation techniques employed during CFIUS reviews.

ICTS Background

Cybersecurity and vulnerabilities in the information technology supply chain have been policy concerns for the U.S. government since at least the Obama administration, with that administration launching the International Strategy for Cyberspace in 2011 and the National Strategy for Global Supply Chain Security in 2012. Nevertheless, such concerns remained firmly in the policy realm until the waning days of the Trump administration.

Specifically, on May 15, 2019, President Donald Trump issued Executive Order No. 13873, which declared a national emergency with respect to ICTS vulnerabilities, authorized Commerce to prohibit certain ICTS transactions and directed Commerce to issue rules further implementing the order.

Although Commerce swiftly issued a proposed rule on Nov. 27, 2019, to implement the executive order, it did not issue a final version of the rule — i.e., the ICTS rule — until the penultimate day of the Trump administration, Jan. 19, 2021.

Notably, the ICTS rule did not become effective until March 22, 2021. Upon assuming office, President Joe Biden ordered a freeze and review of pending regulatory actions that included the ICTS rule. However, unlike other, comparable Trump-era national security measures, the ICTS rule was allowed to go into effect without amendment, suggesting an alignment between the Trump and Biden administration with respect to this policy issue.

The ICTS rule created a new regulatory regime set forth at Title 15 of the Code of Federal Regulations, Part 7. That regime authorizes the secretary of commerce to initiate a review of transactions that (1) involve a person or property subject to the jurisdiction of the U.S.; (2) involve "any property in which any foreign country or national thereof has an interest"; (3) are initiated, pending or completed after the ICTS rule's publication on Jan. 19, 2021; and (4) involve one or more certain specified categories of products.[1]

The ICTS regulations define the products subject to review to broadly include, among other things:

> Software, hardware, or any other product or service integral to data hosting or computing services, to include software-defined services such as virtual private servers, that uses, processes, or retains, or is expected to use, process, or retain, sensitive personal data on greater than one million U.S. persons at any point over the [preceding] twelve (12) months.[2]

Other identified technologies and services include those integral to telecommunications networks, certain mass-market digital technology products and software, and artificial intelligence, advanced computing and advanced robotics.

If a transaction is within the scope of the ICTS rule, it may then be assessed for whether it "involves ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary."[3]

Six governments or persons constitute foreign adversaries for the purposes of the ICTS rule: China, Russia, Cuba, Iran, North Korea and the regime of Nicolás Maduro in Venezuela.

The ICTS rule extends to "any corporation, partnership, association, or other organization organized under the laws" of these six jurisdictions.[4] If the secretary of commerce determines that such a transaction poses "an undue or unacceptable risk," then the secretary may block or require mitigation for the transaction to address the perceived risk.

Buildup to Potential Enforcement

How the ICTS rule will ultimately be enforced in practice remains to be seen and there has been little public action taken by the secretary of commerce under the rule to date. Nevertheless, agency statements, budget information and news reports suggest that Commerce is preparing to exercise its ICTS authority in the near future.

The only enforcement actions publicly acknowledged by Commerce to date have been two rounds of subpoenas. The ICTS rule authorizes the secretary to require persons involved in ICTS transactions to furnish complete information in their custody or control related to the transaction — i.e., to issue administrative subpoenas in connection with reviews of a transaction.[5]

The ICTS rule does not specify at what stage of a review the subpoena may be issued, or the time that a party will have to respond to a subpoena, but the terms of the ICTS rule appear to authorize Commerce to serve subpoenas on third parties.

In March and April 2021, the Department of Commerce announced it had issued subpoenas under the ICTS authority to an unknown number of Chinese companies, but no known further action has been taken.[6] Both press releases noted that the subpoenas were issued

"to support the review of transactions pursuant to Executive Order 13873," but stopped short of identifying the subpoena recipients or acknowledging that any company was under a formal review.

Nevertheless, there has been some public reporting that Commerce is beginning to enforce the ICTS regulations. For example, in January 2022, Reuters reported that Commerce was engaged in a formal review of the cloud business of Chinese e-commerce company Alibaba Group Holding Limited.[7]

Another press outlet reported in March 2022 that Chinese ride-sharing company Didi Chuxing Technology Co. likewise appeared to be the subject of an ICTS review.[8]

More recent budgetary requests also suggest that Commerce is preparing for a coming flurry of ICTS enforcement activity. Specifically, Commerce's proposed budget for the 2023 fiscal year includes a request for approximately $36 million to "secure the national information and communication technology and services (ICTS) supply chain."[9]

The budget request would create 114 new positions dedicated to administration of the ICTS regulations, a dramatic increase over the current 16 positions dedicated to that task. According to the budget:

> This increase will provide a more comprehensive reach to address critical staffing capability gaps required for [Commerce] to evaluate and address national security risks posed by ICTS transactions and to intake and adjudicate licenses, provide a credible enforcement and penalty capability, allow for dedicated legal support for transaction reviews, licenses, and enforcement actions, and correlate complex technical analysis and interpret all-source intelligence (to include cybersecurity threat concerns).[10]

Thus, the agency appears to be preparing for a buildout of its ICTS capabilities.

Preparing for Enforcement Activity

Companies involved in ICTS transactions should therefore begin to proactively prepare for potential enforcement activity by Commerce.

As noted above, companies formed under the laws of the jurisdictions identified as foreign adversaries under the ICTS rule are squarely within the rule's scope. However, other companies that transact with those companies could also face potential enforcement activity.

For example, U.S.-based customers, services providers and other third-party partners of ICTS companies from a "foreign adversary" could receive subpoenas seeking information regarding those ICTS companies.

Although there is a lack of public guidance from Commerce, recent enforcement trends from CFIUS could serve as a guide for companies preparing for ICTS-related action.

There is a high degree of overlap between the government agencies involved in enforcing CFIUS and the Commerce officials responsible for overseeing the ICTS regulations, and in practice, many of the ICTS officials are likely to have experience working on CFIUS.

Mitigation of national security concerns during a CFIUS review is therefore likely to be highly

relevant to similar questions considered during the ICTS process.

Companies potentially at risk for ICTS enforcement action should therefore consider the following steps to prepare.

Develop a response plan.

Companies potentially at risk for ICTS-related enforcement should consider establishing a procedure for responding swiftly to any subpoenas or other inquiries from Commerce. A response plan should, among other things, delegate a preliminary response team, with a chain of command, to enable to company to respond as quickly as possible.

In addition to designating internal stakeholders and subject-matter experts, the plan could include outside resources as well, such as specialized external counsel. Companies may also consider including public relations or lobbying firms to help address any reputational risks from an enforcement action or reduce the risk that Congress may pressure Commerce to take adverse action.

Conduct a risk assessment.

At-risk companies should also consider conducting a risk assessment to identify products or services potentially within the scope of the ICTS rule, and evaluate whether those products or services may raise any national security concerns.

Companies should broadly take into consideration policy statements from Commerce and other U.S. government agencies that may signal likely enforcement priorities. Companies could consider categorizing products and services within the scope of the ICTS rule into high-risk and low-risk groups to better enable the companies to triage any enforcement action.

Proactively mitigate likely concerns.

Depending on the results of the risk assessment, companies should consider ways to mitigate likely national security concerns of Commerce. Taking proactive action to address those concerns even before an investigation is initiated could enable at-risk companies to implement their preferred approach and avoid potential government overreach, and may potentially avoid an enforcement action altogether.

Monitor ICTS developments for guidance.

Although there is currently a lack of public information regarding the ICTS process, at-risk companies should closely monitor industry groups and trade associations for any relevant information that could help to better tailor a response plan.

As more enforcement action is taken, affected companies may be willing to share intelligence on, for example, the information sought by Commerce, the types of companies targeted for subpoenas and any nonpublic guidance or feedback received from Commerce in responding to enforcement action.

Consider applying for a license.

To provide a process for entities to seek pre-approval of their ICTS transactions, Commerce provided in the interim final rule that it would implement and publish procedures for a

licensing process by May 19, 2021.[11] On March 29, 2021, Commerce issued an advance notice of proposed rulemaking seeking public input on such a licensing or other pre-clearance process.

The licensing rule still awaits final action, but the licensing process that is contemplated under the notice is likely to be similar to the process for voluntary pre-transaction filings with CFIUS to obtain a safe-harbor against a future government-initiated review.

If Commerce finalizes the licensing procedures, at-risk companies should consider applying for clearance for in-scope products and services, potentially incorporating proposed mitigating action into their applications.

Conclusion

Much like CFIUS, the ICTS rule and related regulations are a tool for the U.S. government to review and potentially require mitigating action for certain transactions in the U.S. Although the ICTS rule has been in development for nearly two years, Commerce appears to be primed to robustly enforce it in the near future.

Companies from foreign-adversary jurisdictions, as well as their customers and third-party partners, should consider proactively preparing for potential enforcement activity.

Tyler Grove is a partner and John Hannon is an associate at Hughes Hubbard & Reed LLP.

[1] See 15 C.F.R. § 7.3.

[2] See 15 C.F.R. § 7.3(a)(4)(ii)(H)(2).

[3] See 15 C.F.R. § 7.2.

[4] See id.

[5] See 15 C.F.R. § 7.101(a).

[6] Press Release, U.S. Secretary of Commerce Gina Raimondo Statement on Actions Taken Under ICTS Supply Chain Executive Order, Dep't of Com. (Mar. 17, 2021), https://www.commerce.gov/news/press-releases/2021/03/us-secretary-commerce-gina-raimondo-statement-actions-taken-under-icts; Press Release, U.S. Department of Commerce Statement on Actions Taken Under ICTS Supply Chain Executive Order, Dep't of Com. (Apr. 13, 2021), https://www.commerce.gov/news/press-releases/2021/04/us-department-commerce-statement-actions-taken-under-icts-supply-chain.

[7] Alexandra Alper, U.S. Examining Alibaba's Cloud Unit for National Security Risks – Sources, Reuters (Jan. 19, 2022), https://www.reuters.com/technology/exclusive-us-examining-alibabas-cloud-unit-national-security-risks-sources-2022-01-18/.

[8] Ben Brody, A Secretive US Security Program Has its Sights on Didi, Protocol (Mar. 23, 2022), https://www.protocol.com/policy/didi-commerce-icts.

[9] The Department of Commerce Budget in Brief, Fiscal Year 2023, at 67, https://www.commerce.gov/sites/default/files/2022-03/Commerce-FY2023-BIB-Introduction.pdf.

[10] Id. at 70.

[11] See 86 Fed. Reg. 16312 (Mar. 29, 2021).