Articles + Publications | January 23, 2025

Inside New Commerce Tech Restrictions: Key Risk Takeaways

WRITTEN BY

Peter E. Jeydel

This article was originally published on January 23, 2025 on Law360 and is republished here with permission.

The U.S. Department of Commerce's Bureau of Industry and Security has **issued the final rule** that will determine how its Information and Communications Technology and Services regulations will work going forward.[1]

The final rule was published in December and takes effect on Feb. 4. It finalizes the process that BIS' Information and Communications Technology and Services, or ICTS, office will follow as it goes about restricting foreign adversary — largely Chinese — products and technologies in order to protect U.S. national security.

Part 1 of this article provides brief background about the ICTS regulations, and key insights for stakeholders that need to assess their exposure and consider how to mitigate their risk under this emerging regulatory regime.

Part 2 will offer guidance on potential engagement strategies with the ICTS office for those that may be affected by these rules, how the regulatory process will play out and steps that can be taken to enhance compliance with any new ICTS rules that BIS may publish in the future.

Background

This final rule from BIS on the ICTS program does not impose any additional restrictions. Rather, it sets the process that the ICTS office will follow in developing new restrictions and in enforcing the restrictions that it has promulgated, as well as general requirements such as recordkeeping.

A close look at the process formalized in the final rule reveals a great deal about how this new(ish) regulatory program will work.

The ICTS program at BIS stems initially from President Donald Trump's 2019 Executive Order No. 13873, "Securing the Information and Communications Technology and Services Supply Chain," which was then followed by a number of related executive orders.

The Commerce Department, throughout the latter part of the first Trump administration and the entirety of the Biden administration, has been trying to figure out how this expansive regulatory authority should be wielded.

After much engagement with industry and a number of initial rulemakings, BIS has finally issued the final rule setting out in detail how it will administer the ICTS program.

While the structure of the ICTS office and its regulations have been, until now, a work in progress, this group within BIS has already issued an initial set of restrictions, including in June 2024 on Kaspersky Lab's antivirus and cybersecurity products, followed by a proposed rule in September 2024 on certain connected vehicle products from China or Russia.

Most recently, on Jan. 2, 2025, BIS published an advanced notice of proposed rulemaking and request for public comment on ICTS risks relating to unmanned aircraft systems, focusing on the technologies that are "most integral to [unmanned aircraft systems'] data collection and connectivity capabilities and that are most vulnerable to compromise by an adversarial actor."

In finalizing and then enforcing these and future restrictions, BIS will follow the process set out in the ICTS program final rule.

So what should industry make of the final rule that will guide the ICTS office at BIS? It has defined its authority in an extraordinarily broad manner, with such a degree of discretion that any efforts to contest its demands or actions will be highly constrained.

The compliance expectations will be challenging for many companies to meet, and the rules highlight an array of risk areas to consider.

Scope of the Rules

We start with a brief discussion of some of the most critical takeaways regarding the scope and application of the final rule.

CFIUS Carveout (or Lack Thereof?)

The final rule raises serious questions about the real meaning or value of the much-vaunted Committee on Foreign Investment in the United States exception, which has been characterized by some as providing a safe harbor under the ICTS rules for companies that have entered the U.S. market following a successful CFIUS review.

The basic idea is that these companies have already experienced an elbow-deep U.S. government national security review, and therefore deserve a lighter touch under the ICTS regulations.

BIS has confirmed in the final rule that, for "the exception to apply, the ICTS Transaction must be the same transaction that CFIUS" previously reviewed; and that "a separate transaction, even if involving the same transaction parties subject to a CFIUS mitigation agreement, would not be subject to this exception."

BIS added:

The mere fact that an individual or entity has participated in a CFIUS filing or is a party to a CFIUS mitigation agreement would not restrict the Secretary [of Commerce, i.e., BIS] in reviewing any ICTS Transaction to which the individual or entity is party if the ICTS Transaction is distinct from the CFIUS transaction giving rise to a mitigation agreement.

The takeaway from this would be that the value of the CFIUS exception starts to diminish on day one after the CFIUS process has concluded, even if the mitigation terms remain in effect.

Any change to a product or service or other elements may lead BIS to conclude that it is reviewing a distinct transaction, and thus the exception is not applicable.

In another departure from the norm in the CFIUS world, ICTS mitigation agreements may be made public, per the rule.

This is at the discretion of BIS if it finds it "need[s] to inform members of the public about a Final Determination to mitigate risks with the parties to a transaction even if an ICTS Transaction is not prohibited."

These mitigation agreements may of course include highly sensitive information, so companies may contest the public disclosure of certain details.

Numerical Thresholds

The final rule has surprised many observers by doing away with the numerical limitations on personal data and product sales or users that had limited the scope of the proposed rules.

These had been set in many cases at a 1 million-plus threshold. Previously, those limitations had been one of the few ways that companies could determine whether they may be subject to ICTS restrictions.

That is now gone, so even companies with data on just a few U.S. persons can be targeted if the data is sensitive. The same is true for companies with just a few products or users among U.S. persons if they are deemed to present a significant security threat.

This reflects a similar, but even more discretionary, approach as compared to the U.S. Department of Justice's recently finalized "Bulk Sensitive Personal Data and U.S. Government-Related Data" regulations, which the National Security Division will administer.[2]

Broad Restrictive Authority

BIS no longer must use the "least restrictive means" in issuing ICTS prohibitions. Instead, the final rule states that "the Secretary will direct the means that the Secretary determines to be necessary to address the undue or

unacceptable risk."

So again, for parties looking for limitations on the government's authority, keep looking (hint: there aren't many).

Free Services and Technology Transfers

The ICTS office has underscored that even free services such as certain tax or antivirus products can be covered by these rules.

No financial transactions need to occur in order to trigger the ICTS restrictions, as some commenters had suggested. These rules can even cover technology transfers of various types, such as licensing deals and other partnerships, and even intracompany work.

Research, Testing, Standards Development and Other Nonsales Activity

In setting the scope of the term "ICTS transaction," the government has declined to adopt any definition of the term "use" — for example, actual delivery of goods or services to U.S. customers.

Instead, seemingly any activity involving U.S. persons can trigger these rules, even unauthorized "misuses" of a product or technology.

U.S. and Non-U.S. Subsidiaries

The final rule states that, at least "in some cases, … foreign subsidiaries of U.S. companies or U.S. subsidiaries of foreign companies" may be targeted if they have the requisite nexus to a "foreign adversary."

For a non-U.S. subsidiary of a U.S. company, this could be a simple as, according to the final rule, "being required to comply with the rules, laws, or other requirements of that foreign adversary."

Use of Foreign Adversary Software Outside the U.S.

U.S. companies or individuals using software anywhere in the world can be subject to regulation under these rules, if there is a foreign adversary connection and a national security threat.

But the government did state that merely using software in a foreign adversary country would not trigger the rules if it was developed by a company that is not linked to a foreign adversary.

Software Development Collaboration

BIS has stated in the final rule that it can review software "if a U.S. person designed, developed, manufactured, or supplied [it] in collaboration with a foreign adversary-controlled entity" and if the government found that to present a national security risk.

Individuals From Foreign Adversary Countries

In a bit of good news (well, mixed news), the government has clarified that, for U.S. citizens or permanent residents, merely holding dual citizenship or residency in China or another so-called adversary country does not trigger these rules — as under U.S. export controls, discrimination against U.S. persons is not justifiable under these regulations and is to be avoided.

But the flip side is that any non-U.S. person, such as those in the U.S. on a visa or similar status, or third-country citizens and residents, may trigger this rule solely due to their Chinese or other adversary citizenship or residency.

That will present major challenges for the countless technology companies throughout the world that employ such individuals in key roles such as management and product development.

In the same vein, the agency stated in the final rule that "solely employing nationals of a foreign adversary country would not independently trigger an ICTS Transaction review," unless there were "other indicia of ownership, control, or influence by a foreign adversary." That's cold comfort for companies with these individuals in key positions.

Due to the risk and uncertainty, companies should consider conducting a broader security review for certain key personnel, perhaps as part of an export controls screening and compliance process.

This review could be used to show the government that these individuals present no national security risk due to their roles in the company, and that the company's products should not be subject to ICTS restrictions.

No Physical Presence or Physical Products Sold in the U.S.

For companies thinking they are in the clear because of a limited nexus to the U.S., think again. If your product is brought into the U.S. in any manner, even indirectly or purely electronically, you may be within the scope of these rules.

This applies not just to the developer or original equipment manufacturer, but potentially to anyone involved with the product or business: The final rule covers those engaged in "buying, selling, reselling, receiving, licensing, or acquiring ICTS, or otherwise doing or engaging in business involving the conveyance of ICTS."

Macau Included

The final rule clarifies the seemingly obvious point that Macau will be treated as part of China.

Conclusion

The final rule illustrates the breadth and complexity of this emerging regulatory regime that BIS is managing.

While there are a few limitations on its scope that the final rule highlights, BIS retains sweeping authority under the ICTS program to regulate products and technologies linked to foreign adversaries.

---

[1] https://www.bis.gov/press-release/commerce-issues-final-rule-formalize-icts-program.

[2] Justice Department Issues Final Rule Addressing Threat Posed by Foreign Adversaries' Access to Americans' Sensitive Personal Data, Dec. 27, 2024, https://www.justice.gov/opa/pr/justice-department-issues-final-rule-addressing-threat-posed-foreign-adversaries-access.

RELATED INDUSTRIES + PRACTICES

- White Collar Litigation + Investigations
- Sanctions + Trade Controls