Articles + Publications | January 24, 2025

Inside New Commerce Tech Restrictions: Mitigation Strategies

WRITTEN BY

Peter E. Jeydel

This article was originally published on January 24, 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 provided 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 offers 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.

Engaging With the ICTS Office

For technology companies with direct or indirect links to China, Russia, Iran or other designated adversaries of the U.S. — including companies that produce hardware, software or just about anything else — it is important to start thinking about whether or how the ICTS rules may affect the business and how to get ahead of that.

In many cases, the best way to engage with the ICTS office will be in the context of particular subpoenas, proposed restrictions or rulemakings, or other actions, by seeking to narrow or otherwise shape their focus.

Given how broadly BIS has defined its regulatory authority under the ICTS rules, challenging painful restrictions after the fact may not be viable. Therefore, it will often be more effective to focus on policy-level and security-based engagement at as early a stage as possible, such as showing that particular technologies, companies or whatever BIS is targeting do not pose a national security threat, that any such threat can be mitigated, that it can be targeted in a different way, etc.

In certain cases, it may be possible to begin this type of engagement before any action has been taken.

Exclusions

Indeed, the final rule states that the regulators remain "open to considering exclusions if further experience with the rule demonstrates that certain types of ICTS Transactions do not pose an undue or unacceptable risk" to national security. Such categorical exclusions may be an attractive way for particular companies, industry groups, etc. to gain some comfort and certainty in the face of this regulatory authority that is truly daunting in its breadth and potential impact.

No Licensing or Guidance Process — Yet

Beyond the exclusion process, however, certainty on a case-by-case basis may be harder to achieve at this stage, because the long-promised licensing and guidance process is still under consideration.

One can assume BIS is not confident in its ability to handle the number of requests it might receive. BIS' authority could potentially touch the entire global technology ecosystem, which may not be something a handful of people at the Commerce Department can effectively regulate, despite their mandate to do so as best they can.

No Formal Appeals

Similarly, while the agency rejected the proposal for a formal appeals process after restrictions are imposed, it has said it will remain open to requests for reconsideration. So, this will play out at least for now with a somewhat less formal engagement process.

Notice and Comment, and Other Types of Engagement

The ICTS office has also nixed the idea of a public notice-and-comment process prior to finalizing their determinations, i.e., the specific restrictions it will impose. So the process of actually developing prohibitions on particular products, companies, etc. will largely be between the regulators and the targets, and not up for public debate. We saw this with the publication last year of the Kaspersky rules.

BIS has adopted this approach due to concerns about anticompetitive behavior if the process were more open — e.g., the risk that companies may throw competitors under the bus by claiming their products are compromised or insecure. Of course, there were also other reasons, including the massive paperwork burden that an additional notice-and-comment process would impose, as well as a desire for confidentiality in the highly sensitive back-and-forth with targets about the national security threats they may pose.

Clearly, though, there is a risk that, by keeping the determination process behind closed doors, regulators may fail to understand key market dynamics, technological issues, etc., and may misfire with some of their rulemakings. So, while there may not be a formal notice-and-comment process for ICTS determinations, stakeholders should nonetheless follow developments closely and consider effective strategies for engagement.

Tattling on Competitors — And Leads From Watchdog Groups

At the same time, companies at risk should consider how those that may have an axe to grind may unexpectedly

throw them into the ring with the ICTS office.

Companies should be watchful of the possibility that competitors, nongovernmental organizations or similar watchdogs, or others may make a referral about them to BIS. The final rule states that the ICTS office "would not reject that information" if it would assist their review.

But the agency did take the opportunity to put out a bit of a warning about any such action that could be viewed as an "abuse of its processes for anti-competitive purposes." So, far from being a free-for-all, BIS "will carefully vet information provided voluntarily by private industry."

However, the agency declined to adopt a process for accused parties to have a chance to review and respond to reports made against them, or even any requirement for private accusers to provide a sworn affirmation that the information supplied is true and correct — although BIS noted that false statements may be penalized.

While affected parties will be able to see and respond to "the factual basis supporting" a determination once it has been proposed, the government will keep many of its cards close to its chest. Parties may not receive full disclosure of the sources of information such that their credibility or biases can be assessed.

Publication of Initial Determinations

Parties will have serious concerns about how meaningful the due process protections in these rules are, given that the government can go ahead and publish its initial determination before the full process has had a chance to play out.

BIS said, recognizing "that there may be an economic impact on parties named in those publications," that the agency "may choose not to publish" them. Or they may publish them. Of course, for companies concerned about their reputations, or hoping for a fair process, this discretion may be deeply worrying.

Limited Confidentiality

The ICTS office underscored that it may disclose confidential information provided to it, based on a request from a non-U.S. government, if necessary for national security purposes. It also appears to have reserved the right to disclose confidential information publicly if necessary to prevent imminent harm to U.S. national security or the security and safety of U.S. persons.

So one should not have a misplaced sense of great comfort about the confidentiality of the highly sensitive information that will be extracted by the government when going through this process.

Interagency Consensus — Just a Mirage?

The final rule sets out a short timeline for other U.S. government agencies to provide input while ICTS determinations are under consideration, and creates a presumption that other agencies either agree or have no input if they do not weigh in on time. This may essentially empower BIS to move forward unilaterally in such cases.

Given the complexity of ICTS reviews, the very short two- or three-week timelines for senior-level input from other agencies may prove to be unrealistic. Even if another agency does disagree, BIS appears to take the position that it can in effect just note that and move on.

BIS says it will carefully consider any such objection. Perhaps revealing its bottom-line view, BIS notes that "E.O. 13873 does not require the Secretary to seek consensus." So, while finding allies elsewhere in the U.S. government may absolutely help, at the end of the day it is clear where one must bend the knee.

Compliance and Risk Mitigation Pointers

The final rule provides a few important insights for stakeholders on mitigating the risk of being targeted by the ICTS office, and on promoting compliance once targeted — or otherwise affected because of a business relationship with a target.

No Individual Notice Provided

BIS acknowledged its actions when reviewing and restricting specific products may have an impact on countless parties, "many of whom cannot be individually identified." In such cases, the rule notes that serving notice of a determination "on every party may not be feasible or may be unnecessary or inappropriate." What this means is essentially all parties operating with a connection to U.S. persons and U.S. adversaries should try as best they can to monitor the ICTS developments in order to remain in compliance with new restrictions as they emerge.

Third Parties Can Be Penalized

Despite the lack of individual notice, the final rule states that any party can be penalized for violating restrictions established under the ICTS authorities, even for violating another party's mitigation terms, and even if the violator was not involved in the review or other process with BIS.

However, BIS did clarify in the final rule that a knowledge requirement will apply in some cases, such as "assisting a violation" of a mitigation agreement. The "knowledge" standard here is the same as under BIS' export control regulations. What this means in practice is that there's an expectation to review the ICTS rules as they are published and maintain compliance with them in a reasonable, risk-based manner.

Indefinite Restrictions, Retroactivity, Recordkeeping — And Broader Implications

The final rule states that the restrictions and mitigation obligations under the ICTS regime may be imposed for an indefinite period, with no obligation on the part of the government to review the situation periodically. But the government will be allowed to change the requirements at any time. BIS said: "In some cases, a mitigation measure might be appropriate for a limited time; in other cases, a limited time frame might merely delay the realization of the identified risks or even increase them."

But if targeted parties violate mitigation terms, a previously permitted transaction may subsequently be prohibited. These rules will be spelled out in individual determinations and mitigation agreements.

With what may be viewed as a bit of a sleight of hand, the government has stated that the “final rule does not apply retroactively to transactions that were completed prior to January 19, 2021.”

What a relief … until one looks more closely, where it states that, nevertheless, it “may review ICTS Transactions initiated, pending, or completed on or after January 19, 2021, even if they are related to a contractual or other agreement established prior to January 19, 2021.” So in essence, any ongoing activity can be targeted, and there will be little or no grandfathering. With a refreshingly forthright attitude, BIS acknowledged that “the regulations could change expectations about how parties’ multi-year arrangements would operate relative to before the rule took effect.” That may be an understatement.

Layered on top of this, rather than the previously proposed indefinite record retention requirement, there is now a — still very long — 10-year recordkeeping requirement, although BIS retains the discretion to require a longer period of record retention in particular cases. This notably goes beyond the general five-year U.S. export control recordkeeping requirement, and now matches the recently expanded 10-year U.S. sanctions recordkeeping expectation.

Beyond the challenge of implementing a 10+ year recordkeeping requirement for many organizations, not to mention how to define the scope of that for such an amorphous regulatory regime as this, it is worth stepping back and considering what the agency is conveying with these rules.

Conclusion

The ICTS regulations can essentially restrict any products or technologies brought into the U.S. or used by U.S. persons in any manner if they have some link to China or other foreign adversaries, and are viewed as presenting a national security risk.

The 10+ year record retention rule, retroactivity and other elements illustrate that generally there is no safe harbor or similar comfort that companies can obtain, even if they have been in the U.S. market for years — unless, as noted above, they can extract from the agency an exclusion that would cover them, or if they never make changes to their business following a successful review by the Committee on Foreign Investment in the U.S. In this rulemaking, the agency states that its focus areas “are not always correlated with the transaction’s scale and exist regardless of where or when the ICTS enters into the ICTS supply chain.”

The final rule presents a daunting picture for companies and other stakeholders that may be affected by the ICTS regulations. BIS has made clear that it interprets its authority under the ICTS program very broadly, and retains considerable discretion in how it will apply these rules.

Those that may fall within the ICTS office’s crosshairs, or that may be indirectly affected by this emerging regulatory regime, should develop an effective strategy for assessing and mitigating the risks they will face, as additional rules are published and as BIS begins to pursue enforcement actions.

Companies concerned about how these rules may affect them should develop current, historical and forward-looking reviews of products, security, compliance, links to foreign adversaries and other elements, with an eye on assessing and addressing any risks to their business under the ICTS rules.

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

RELATED INDUSTRIES + PRACTICES

- White Collar Litigation + Investigations
- Sanctions + Trade Controls