Debevoise National Security Update: Department of Commerce Issues First Final Determination under ICTS Regime

June 25, 2024

On June 20, 2024, U.S. Department of Commerce's Bureau of Industry & Security ("BIS") issued its first Final Determination under the Information and Communications Technology and Services ("ICTS") Supply Chain Rule, targeting Kaspersky Lab, Inc., the U.S. subsidiary of a Russia-based anti-virus software and cybersecurity company, and its affiliates, subsidiaries, and parent companies ("Kaspersky").[1] The Final Determination prohibits Kaspersky from providing certain anti-virus products and services in the United States or to U.S. persons, wherever located, and also prohibits, in the United States or by U.S. persons, the resale of Kaspersky cybersecurity or anti-virus software, integration of Kaspersky cybersecurity or anti-virus software into other products and services, or licensing of Kaspersky cybersecurity or anti-virus software for purposes of resale or integration into other products or services.

This move follows our expectation, as discussed in the *Debevoise National Security Update: Supply Chain Security in 2024*,[2] that the Commerce Department intends to enhance ICTS enforcement in the near term. This client alert addresses the implications of the Final Determination and ICTS enforcement more generally, including for companies that have a nexus with ICTS suppliers, namely those located in, owned or controlled by, or subject to the jurisdiction of, a "foreign adversary," such as China or Russia.

BACKGROUND: DEPARTMENT OF COMMERCE'S ICTS REGIME

On May 15, 2019, the Trump Administration issued Executive Order 13873 to strengthen efforts to prevent certain countries designated by BIS as foreign adversaries, including China and Russia, from exploiting vulnerabilities in the nation's ICTS supply

---

1 *See Commerce Department Prohibits Russian Kaspersky Software for U.S. Customers*, bis.gov (June 20, 2024), available at https://www.bis.gov/press-release/commerce-department-prohibits-russian-kaspersky-software-us-customers.

2 *See Debevoise National Security Update: Supply Chain Security in 2024*, debevoise.com (March 11, 2024), available at https://www.debevoise.com/insights/publications/2024/03/debevoise-national-security-update-supply-chain.

chain.[3] Implementing regulations were issued by the Commerce Department on January 19, 2021 (the "Supply Chain Rule"), prohibiting certain transactions that involve ICTS "designed, developed, manufactured, or supplied by persons, owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries," whenever the Secretary of Commerce, in consultation with other federal officials, determines that such a transaction, or a class of transactions, poses an undue or unacceptable risk to U.S. national security (each, an "ICTS Transaction").[4] The Supply Chain Rule broadly defines the scope of covered ICTS Transactions to include, among other things, ICTS used by critical infrastructure, integral to certain network or communications systems, related to sensitive personal data of U.S. individuals, enabling of internet communications, or is integral to certain sensitive technologies, including AI, quantum computing, drones or robotics.[5]

This Final Determination is only the second significant action under the Supply Chain Rule and follows an Advanced Notice of Proposed Rulemaking ("ANPRM") by BIS issued on February 29, 2024, that seeks information about potential vulnerabilities in ICTS integral to "connected vehicles" that could result from access to related systems or data by a "foreign adversary."[6]

THE KASPERSKY FINAL DETERMINATION

The Kaspersky Final Determination is the first ICTS Transaction that BIS has prohibited under the ICTS regime. BIS found that Kaspersky's software products – banned from use within U.S. federal agencies since 2017[7] – serviced over 400 million users and 270,000 corporate clients globally, and that:

- Kaspersky is subject to the jurisdiction of the Russian government and must comply with requests for information that could lead to the exploitation of access to sensitive information present on electronic devices using Kaspersky's anti-virus software;

---

[3] *See Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain*, federalregister.gov (May 15, 2019), available at https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain; 15 C.F.R. Part 7.

[4] 15 C.F.R. §§ 7.1, 7.100.

[5] 15 C.F.R. § 7.3(a)(4)(i).

[6] *See Citing National Security Concerns, Biden-Harris Administration Announces Inquiry into Connected Vehicles*, commerce.gov (Feb. 29, 2024), available at https://www.commerce.gov/news/press-releases/2024/02/citing-national-security-concerns-biden-harris-administration-announces.

[7] *See DHS Statement on the Issuance of Binding Operational Directive 17-01*, dhs.gov (Sept. 13, 2017), available at https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01.

- Kaspersky has broad access to, and administrative privileges over, customer information through the provision of cybersecurity and anti-virus software, meaning that Kaspersky employees could potentially transfer U.S. customer data to Russia (where it would be accessible to the Russian government);

- Kaspersky has the ability to use its products to install malicious software on U.S. customers' computers or selectively deny updates; and

- Kaspersky software is integrated into third-party products and services through resale of its software into other products and services, which increases the likelihood that Kaspersky software could be introduced into devices or networks containing highly sensitive U.S. persons data.[8]

The ban goes into effect in two stages on July 20 and September 29, 2024. Beginning on July 20, 2024, Kaspersky will be prohibited from entering into any new agreement with U.S. persons involving one or more ICTS transactions. Then, beginning September 29, 2024, Kaspersky, with respect to all U.S. persons, will be prohibited from providing any anti-virus signature updates and codebase updates (including for software already in use) and must cease operation of the Kaspersky Security Network. Also beginning on that date, the Final Determination prohibits, in the United States or by U.S. persons, the resale of Kaspersky cybersecurity or anti-virus software, integration of Kaspersky cybersecurity or anti-virus software into other products and services, or licensing of Kaspersky cybersecurity or anti-virus software for purposes of resale or integration into other products or services.[9] Violations of the ban could lead to steep civil and criminal penalties: civil penalties can be the greater of $250,000 or twice the amount of the transaction that is the basis of the violation, while criminal penalties can include fines for as much as $1,000,000 and imprisonment for up to 20 years.[10] The Final Determination does not prohibit the continued use of Kaspersky products solely for internal purposes although BIS strongly encourages a transition to alternative services.

---

[8] *See supra* n. 1; *Kaspersky Lab, Inc. Prohibition*, oicts.bis.gov (June 20, 2024), available at https://oicts.bis.gov/kaspersky/.

[9] A non-exhaustive list of products and services covered by the Final Determination is available at *Commerce Department Prohibits Russian Kaspersky Software for U.S. Customers*, *Appendix B* (June 20, 2024), https://oicts.bis.gov/pdfs/AppendixB.pdf. The Final Determination does not prohibit transactions involving, for example, threat intelligence products and services or consulting and advisory services that are informational or educational in nature.

[10] *See* 15 C.F.R. § 7.200.

KEY TAKEAWAYS

The issuance of the first Final Determination under the ICTS Supply Chain Rule—more than five years after Executive Order 13873—is significant. It confirms that BIS is increasing its enforcement actions and focusing on cybersecurity and connected software (via its ANPRM) in the first instance. Moreover, the Commerce Department has requested more than $30 million in FY25 budget increases for BIS, including for ICTS enforcement.[11]

Companies can prepare for increased enforcement by:

- **Inventorying Existing ICTS Applications for Kaspersky Products**. U.S. companies should inventory their ICTS applications to identify whether they utilize Kaspersky products, and if so, diversify their supply chains and seek alternative cybersecurity providers.

- **Evaluating the Significant Business Risk Posed by Transacting With Kaspersky or Including Kaspersky Products in the Company's Own Products or Services**. While the Final Determination does not prohibit companies that already utilize Kaspersky products solely for their own internal purposes from continuing to do so, companies that either do business with Kaspersky regarding software produces or include such Kaspersky products in their own products or services are at significant risk of violating the Final Determination, which can carry steep civil and criminal penalties.

- **Conducting Due Diligence on Other ICTS Suppliers under the Jurisdiction of a BIS-Designated "Foreign Adversary."** As noted, we expect additional enforcement by BIS. In preparation for this, companies should consider a related risk assessment that reviews ICTS suppliers from any "foreign adversaries," including China (including Hong Kong), Cuba, Iran, North Korea, Russia, and the Maduro Regime in Venezuela.

- **Developing a Supply Chain Mitigation and Response Plan**. Potentially affected companies should consider a response plan to mitigate the risk of operational disruption should BIS take action against an ICTS supplier in the company's supply chain.

---

[11] *See U.S. Department of Commerce, Bureau of Industry and Security: Fiscal year 2025 President's Budget Request*, commerce.gov, available at https://www.commerce.gov/sites/default/files/2024-03/BIS-FY2025-Congressional-Budget-Submission.pdf.

- **Integrating ICTS Considerations into Merger and Acquisition Due Diligence.** Companies should consider whether potential targets present enhanced ICTS risks as part of their merger and acquisition due diligence (e.g., to identify whether the target utilizes Kaspersky software or any other ICTS products banned in the future).

* * *

Please do not hesitate to contact us with any questions.

Catherine Amirfar
Partner, New York
+1 212 909 7423
camirfar@debevoise.com

Luke Dembosky
Partner, Washington, D.C.
+1 202 383 8020
ldembosky@debevoise.com

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com

Erez Liebermann
Partner, New York
+1 212 909 6224
eliebermann@debevoise.com

Rick Sofield
Partner, Washington, D.C.
+1 202 383 8054
rcsofield@debevoise.com

Robert T. Dura
Counsel, Washington, D.C.
+1 202 383 8247
rdura@debevoise.com

Isabelle Glimcher
Associate, New York
+1 212 909 6542
iwglimcher@debevoise.com

Gabriel A. Kohan
Associate, Washington, D.C.
+1 202 383 8036
gakohan@debevoise.com

Stephanie D. Thomas
Associate, New York
+1 212 909 6535
sdthomas@debevoise.com