SQUIRE PATTON BOGGS

Commerce Issues First "Final Determination" Under ICTS Supply Chain Rules, Banning Kaspersky Software Products From US Commerce

US – June 2024

On June 20, 2024, the Department of Commerce's Bureau of Industry and Security (Commerce) announced the issuance of the first Final Determination (Determination) under Executive Order 13873 – Securing the Information and Communications Technology and Services (ICTS) Supply Chain.

The Determination, which was published in the Federal Register on June 24, 2024, imposes a prohibition on transactions by Russian-affiliated Kaspersky Lab Inc. (together with all affiliates, subsidiaries, and parent companies) (Kaspersky) involving the "provision of cybersecurity and anti-virus software and related services to persons subject to the jurisdiction of the United States" (Kaspersky Transactions).

Executive Order 13873 and ICTS Supply Chain Regulations

Executive Order 13873, which dates back to the Trump administration and is implemented in 15 C.F.R. Part 7 (ICTS Rule), authorizes the Secretary of Commerce (Secretary) to review certain transactions to "determine (1) whether those transactions are covered ICTS transactions; and if so, (2) whether those transactions pose an undue or unacceptable risk to U.S. national security or the safety and security of U.S. persons." (A summary of what constitutes a covered ICTS transaction, and the review process under the ICTS Rule, is provided in our insight from the time of the regulations' publication.)

Commerce's ICTS Investigation Into Kaspersky

The review process under Executive Order 13873 is triggered by a "referral" (see 15 C.F.R. § 7.103(a)), which can come from various sources as well as the Secretary's own decision. In this case, the Department of Justice (DOJ), in August of 2021, requested that Commerce review the Kaspersky Transactions. Commerce first determined that the transactions were "covered ICTS transactions" pursuant to the applicable criteria (e.g., the transactions involve ICTS designed, developed, manufactured or supplied by persons owned by, controlled by or subject to the jurisdiction or direction of a foreign adversary). (This summary chart explains the six ICTS categories subject to the ICTS Rule.) Commerce then issued a subpoena to Kaspersky in May of 2022 as the next phase of the investigation.

After analyzing the materials Kaspersky produced, as well as other information, and engaging in the required interagency consultation process, Commerce issued an initial determination on October 5, 2023, which recommended that Commerce prohibit certain covered ICTS transactions involving Kaspersky cybersecurity and antivirus software. As permitted under the ICTS Rule, Kaspersky was allowed to respond, including challenging the factual basis for the initial determination and proposing certain mitigation measures; the response was submitted by Kaspersky on January 3, 2024.

Commerce nevertheless concluded in the Determination that the prohibition proposed in the initial determination was "well supported," pointing to the following risks:

- **Jurisdiction, control, or direction of the Russian government** – 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 antivirus software.
- **Access to sensitive US customer information through administrative privileges** – Kaspersky has broad access to, and administrative privileges over, customer data through the provision of its cybersecurity and antivirus software. Kaspersky employees could potentially transfer US customer data to Russia, where it would be accessible to the Russian government under Russian law.
- **Capability or opportunity to install malicious software and withhold critical updates** – Kaspersky has the ability to use its products to install malicious software on US customers' computers or to selectively deny updates, leaving US persons and critical infrastructure vulnerable to malware and exploitation.
- **Third-party integration of Kaspersky products** – Kaspersky cybersecurity or antivirus software is integrated into third-party products and services, increasing the likelihood that Kaspersky software could unwittingly be introduced into devices or networks containing highly sensitive US persons' data.

Additional information considered by Commerce in reaching the Determination is set forth, albeit in redacted fashion, in Appendix A to the Determination.

The Final Determination – Banning Kaspersky ICTS Products and Services

The Determination prohibits Kaspersky from engaging in certain covered ICTS transactions involving (a) any cybersecurity product or service designed, developed, manufactured or supplied, in whole or in part, by Kaspersky, (b)any antivirus software designed, developed, manufactured or supplied by Kaspersky and (c) the integration of software designed, developed, manufactured or supplied, in whole or in part, by Kaspersky into third-party products or services (e.g., ''white-labeled'' products or services). Included are those products listed on Appendix B to the Determination.

The Determination's prohibition will be effective on July 20, 2024, with respect to Kaspersky entering into new agreements for the covered ICTS transactions. However, to minimize disruption to US consumers and businesses and to give them time to find suitable alternatives, the Determination allows Kaspersky to continue certain operations in the US – including providing antivirus signature updates and codebase updates – until September 29, 2024.

The Determination does not affect transactions involving Kaspersky Threat Intelligence products and services, Kaspersky Security Training products and services, or Kaspersky consulting or advisory services (including SOC Consulting, Security Consulting, Ask the Analyst and Incident Response) that are purely informational or educational in nature.

Additional Restrictions Imposed on Kaspersky

Such restrictions and prohibitions are not new for Kaspersky. As Commerce noted, "In 2017, the Department of Homeland Security issued a directive requiring federal agencies to remove and discontinue use of Kaspersky-branded products on federal information systems. Additionally, the National Defense Authorization Act (NDAA) for Fiscal Year 2018 prohibited the use of Kaspersky by the federal government. In addition, in March 2022, the US Federal Communications Commission added to its 'List of Communications Equipment and Services that Pose a Threat to National Security' information security products, solutions and services supplied, directly or indirectly, by Kaspersky."

Further, in addition to the Determination, Kaspersky entities and individuals in leadership roles were added to restricted party lists. Commerce added three Kaspersky entities – AO Kaspersky Lab and OOO Kaspersky Group (Russia), and Kaspersky Labs Limited (UK) – to the Bureau of Industry and Security's Entity List for their cooperation with Russian military and intelligence authorities in support of the Russian government's cyber intelligence objectives. And a dozen "individuals in executive and senior leadership roles at AO Kaspersky Lab" were added to the Specially Designated Nationals List administered by the Office of Foreign Assets Control of the Treasury Department.

Process Considerations

The Determination may provide a road map for others to come, particularly in terms of timing. The timeline for the Kaspersky investigation played out as follows:

Event	Date
Referral from DOJ to Commerce	August 25, 2021
Administrative ICTS subpoena	May 25, 2022
Initial determination by Commerce	October 5, 2023
Response to initial determination	January 3, 2024
Final Determination	June 21, 2024

This shows a nearly three-year process, with approximately nine months of review before issuing a subpoena, nearly 17 months before issuing an initial determination, and almost six months to come to a final determination after receiving a response to an initial determination.

Commerce generally does not publicly identify what referrals it might be considering for investigation. However, in March of 2021, Commerce announced that it had served multiple subpoenas on Chinese companies that provide ICTS in the US; however, to date, there have been no final determinations as a result.

Contacts

Paul C. Besozzi
Senior Partner, Washington DC
T +1 202 457 5292
E paul.besozzi@squirepb.com

Peter C. Alfano III
Partner, Washington DC
T +1 202 626 6263
E peter.alfano@squirepb.com

Robert E. Stup, Jr.
Partner, Washington DC
T +1 202 626 6721
E robert.stup@squirepb.com

George N. Grammas
Partner, Washington DC
T +1 202 626 6234
E george.grammas@squirepb.com

Daniel E. Waltz
Senior Partner, Washington DC
T +1 202 457 5651
E daniel.waltz@squirepb.com

Karen R. Harbaugh
Partner, Washington DC
T +1 202 457 6485
E karen.harbaugh@squirepb.com