Now & Next

Export Controls Alert

June 24, 2024

BIS's OICTS issues first Final Determination prohibiting Russian Kaspersky software for US customers

By David Crosby, Christopher Grigg, Alexandra López-Casero, and Jule Giegling[i]

BIS recommends that individuals and businesses that utilize Kaspersky software transition to new vendors.

What's the impact?

- This Kaspersky Labs Prohibition is the first action by BIS's Office of Information and Communications Technology and Services (OICTS).
- Kaspersky will no longer be able to sell its software within the United States or provide updates to software already in use.
- However, US users will not face civil or criminal penalties if they continue to use Kaspersky's products but should be aware that Kaspersky will no longer be allowed to provide signature updates needed for effective anti-virus protection after 12:00 am ET on September 29, 2024.

On June 20, 2024, the Department of Commerce's Bureau of Industry and Security (BIS) announced a Final Determination prohibiting Kaspersky Lab, Inc., the US subsidiary of a Russia-

based anti-virus software and cybersecurity company, from directly or indirectly providing anti-virus software and cybersecurity products or services in the United States or to US persons. The prohibition also applies to Kaspersky Lab, Inc.'s affiliates, subsidiaries, and parent companies (together with Kaspersky Lab, Inc., "Kaspersky"). This action is the first of its kind, as it is the first use of the Commerce Department's Information and Communications Technology and Services (ICTS) authority and the first Final Determination issued by OICTS, whose mission is to investigate whether certain information and communications technology or services transactions in the United States pose an undue or unacceptable national security risk. Following this Final Determination, Kaspersky will generally no longer be able to sell its software within the United States or provide updates to software already in use.

In addition to the Final Determination, BIS designated three of Kaspersky's entities, namely the Russian entities AO Kaspersky Lab and OOO Kaspersky Group and the UK entity Kaspersky Labs Limited, on its Entity List for their cooperation with Russian military and intelligence authorities in support of the Russian government's cyber intelligence objectives. The designations will become effective upon formal publication scheduled for June 24, 2024. Furthermore, OFAC designated twelve individuals in executive and senior leadership roles at AO Kaspersky Lab on June 21, 2024, effective immediately.

The June 20, 2024, OICTS Final Determination

The Final Determination was issued under the authority granted in Executive Order (EO) 13873, "*Securing the Information and Communications Technology and Services Supply Chain*." This EO empowers the Department of Commerce to investigate whether certain ICTS transactions (1) pose an undue or unacceptable risk of sabotage to or subversion of ICTS in the United States; (2) pose an undue risk of catastrophic effects on the security or resiliency of US critical infrastructure or the digital economy of the United States; or (3) otherwise pose an unacceptable risk to the national security of the United States or the security and safety of US persons. If the Department of Commerce determines that an ICTS transaction poses an undue or unacceptable risk, it may, in consultation with its interagency partners, prohibit the transaction or impose mitigation measures. This authority is exercised by BIS, specifically OICTS.

Following an August 2021 referral by the Department of Justice, OICTS reviewed transactions involving Kaspersky's provision of cybersecurity and anti-virus software and related services to persons subject to the jurisdiction of the United States. OICTS found that the provision of these products to US persons, including through third-party entities that integrate Kaspersky cybersecurity or anti-virus software into commercial hardware or software, poses "*undue and unacceptable risks to U.S. national security and to the security and safety of U.S. persons*." As a consequence, OICTS, through the Final Determination, prohibited Kaspersky from conducting or participating in certain ICTS transactions with US persons. These include transactions involving:

- Any cybersecurity product or service designed, developed, manufactured, or supplied, in

whole or in part, by Kaspersky with respect to specific products and services;

- Any anti-virus software designed, developed, manufactured, or supplied, in whole or in part, by Kaspersky with respect to specific products and services; and
- 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-labelled" products or services).

Also prohibited is any resale, integration 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, either in the United States or by US persons. OICTS specified the products and services encompassed by these prohibitions in a non-exhaustive list (here is the full list of prohibited transactions).

The national security risks OICTS identified stem from the potential for Kaspersky products to be used strategically to cause harm to the United States. As an entity subject to Russian jurisdiction, Kaspersky must comply with any Russian government information or assistance requests. Russian laws compel companies subject to Russian jurisdiction to cooperate with Russian intelligence and law enforcement efforts, including requests from the Russian Federal Security Service. Kaspersky's technical engineers have detailed knowledge of vulnerabilities and backdoors that may exist in the software operating on US person devices. Additionally, Kaspersky may modify the software on a user's device to reroute the transmission of data collected by the device, potentially including personal and proprietary user data, to Kaspersky servers located in Russia or otherwise accessible from Russia. Furthermore, the Kaspersky Security Network (KSN) function built into the software can send data about users' suspicious files or applications through the KSN for analysis based on certain Kaspersky-identified threat indicators. OICTS further considered that integration of Kaspersky software into third-party hardware or software or any "white labeling" of Kaspersky software further poses a risk as users would be less likely to know the true source of the code.

Effective dates

The prohibitions will take effect in two stages.

Beginning 12:00 am ET on **July 20, 2024**, Kaspersky will be prohibited from entering into any new agreement with US persons involving one or more of the transactions identified above.

Beginning 12:00 am ET on **September 29, 2024**, Kaspersky and any of its successors or assignees will be prohibited from:

- Providing any anti-virus signature updates and codebase updates associated with the ICTS transactions identified above; and
- Operating the Kaspersky Security Network (KSN) in the United States or on any US person's

information technology system.

Also prohibited, effective 12:00 am ET on **September 29, 2024**, is *any* resale, integration into other products and services, and licensing of Kaspersky cybersecurity or anti-virus software for purposes of resale or integration into other products or services.

The Final Determination does not apply to 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.

Kaspersky

Kaspersky provides IT security solutions, including tools for defense against cyberthreats, such as malware, spam, hackers, distributed denial of services attacks, cyber espionage tools, and cyber weapons that target critical infrastructure, to home computer users, small companies, large corporations, and governments. Kaspersky is a multinational company with offices in 31 countries, servicing 400 million users and 270,000 corporate clients in over 200 countries and territories.

Kaspersky has been subject to US Government action before. In 2017, the Department of Homeland Security issued a directive requiring federal agencies to remove and discontinue the use of Kaspersky-branded products on federal information systems. The National Defense Authorization Act for Fiscal Year 2018 prohibited the use of Kaspersky by the federal government. In addition, in March 2022, the US Federal Communications Commission added information security products, solutions, and services supplied, directly or indirectly, by Kaspersky to its "*List of Communications Equipment and Services that Pose a Threat to National Security.*"

Legal implications

The Final Determination imposes a prohibition globally on Kaspersky concerning its provision of specified products and services to any US person. It is important to note that this prohibition does not expose the users of Kaspersky's products to the risk of civil or criminal penalties. Specifically, US persons will not face enforcement actions by the Department for the continued use of Kaspersky products obtained prior to the issuance of the Final Determination. However, US persons are advised to seek alternative products, as Kaspersky will no longer be allowed to provide signature updates needed for effective anti-virus protection after 12:00 am ET on September 29, 2024. Further, while US persons may continue to use Kaspersky products after the effective date, they should consider whether the continued use of Kaspersky products would breach their cybersecurity insurance policies or subject them to negligence claims in the event of a cybersecurity incident.

Practical impact

This is the first action by OICTS under the new ICTS regulations, and the first action, specifically, targeting the cyber-security supply chain. With the US government increasingly paying attention to cyber security, we expect more actions targeting this and other computer-technology-related areas to be issued in the near future.

BIS recommends that individuals and businesses using Kaspersky software transition to new vendors to limit exposure of personal or other sensitive data to malignant actors due to a potential lack of cybersecurity coverage. BIS is currently working with the Department of Homeland Security and Department of Justice to inform US customers, including state, local, tribal, and territorial (SLTT) government agencies, non-government customers at the SLTT level, and critical infrastructure operators, about ways to easily remove the software. In addition, the Department is working with federal departments and agencies to inform users about this action.

Additional information about this action and publicly available resources can be found on OICTS's website and Frequently Asked Questions (FAQs) page. The text of the Final Determination and a non-exhaustive list of prohibited products and services are available in the *Federal Register*.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

David F. Crosby
617.345.1264
dcrosby@nixonpeabody.com

Christopher D. Grigg
213.629.6134
cgrigg@nixonpeabody.com

Alexandra López-Casero
202.213.0171
alopezcasero@nixonpeabody.com

---

[i] Jule Giegling (Legal Intern–Corporate Practice) assisted with the preparation of this alert.