MAYER | BROWN

25 JUNE 2024

BIS ISSUES FIRST ICTS BAN, PROHIBITING SALES AND UPDATES TO KASPERSKY PRODUCTS AND SERVICES IN THE US, WHILE OFAC SANCTIONS SENIOR EXECUTIVES AND DIRECTORS

AUTHORS: ADAM S. HICKEY, TAMER A. SOLIMAN, HOWARD W. WALTZMAN, AARON FUTERMAN

On June 20, 2024, the Department of Commerce's Bureau of Industry and Security (BIS) issued a Final Determination ("Determination") prohibiting Kaspersky Lab, Inc.—the US subsidiary of the Russia-based antivirus software and cybersecurity company—from directly or indirectly providing antivirus software and cybersecurity products or services in the United States or to US persons. The Determination is the first issued under the Department's Information and Communications Technology and Services (ICTS) authorities pursuant to Executive Order 13783, permitting it to prohibit or restrict ICTS transactions with a direct or indirect nexus to certain designated "foreign adversaries" (notably including Russia and China) to protect US national security. The Determination not only affects US companies using or otherwise dealing in Kaspersky software (as well as designated individuals or entities), but also highlights risks for companies (regardless of sector) whose supply chain includes ICTS designed, developed, or supplied by persons with a "foreign adversary" nexus.

In connection with the Determination, BIS added three key Kaspersky entities to the Entity List, thereby prohibiting their access to US goods, software, and technology; and the Treasury Department's Office of Foreign Assets Control (OFAC) imposed economic sanctions on twelve individual board members and senior executives of Kaspersky. We discuss these developments and their implications for US and non-US companies below.

BACKGROUND

BIS issued the Determination pursuant to its authority under Executive Order 13873 of May 15, 2019, which declared a national emergency stemming from "foreign adversaries . . . increasingly creating and exploiting vulnerabilities" in ICTS supply chains.[1] As discussed in our prior Legal Updates on the ICTS framework and implementing regulations, that Order delegates broad authority to Commerce—in consultation with other agencies—to restrict, impose mitigation measures on, or potentially unwind, transactions or categories of transactions involving ICTS with ties to a "foreign adversary" that pose undue or unacceptable risks to US national security or US persons. Since 2019, Commerce has publicly confirmed that it was conducting several investigations under this new authority, including several referred by the Department of Justice. Commerce also established, and rapidly grew, an office within BIS dedicated to the implementation and enforcement of its ICTS authority. However, prior to this action, Commerce had yet to publish any determinations or restrictive measures on any ICTS transaction or category of transactions under that authority. The decision to fully ban Kaspersky cybersecurity and antivirus products in the United States

follows a 2017 Department of Homeland Security directive banning the use of the same Kaspersky products by federal government agencies. At that time, news outlets reported ties between Kaspersky and Russian intelligence services, including that Russian hackers had used Kaspersky software to steal classified material from the computer of a National Security Agency (NSA) contractor.

THE ICTS DETERMINATION

Beginning on July 20, 2024, the Determination prohibits Kaspersky from entering any new agreement with US persons involving transactions for any cybersecurity product or service, anti-virus products and services, and integration of software designed or supplied by Kaspersky into third-party products and services. And as of September 29, 2023, Kaspersky is prohibited from providing any updates for its products and from operating the Kaspersky Security Network (KSN) in the US. In addition, the Determination prohibits reselling, integrating, or licensing Kaspersky cybersecurity or anti-virus software. The Determination does not apply to Kaspersky Threat Intelligence products and services, Security Training products and services, or consulting or advisory services.

US individuals and companies that still rely on Kaspersky products and services should immediately seek alternative products and services, and completely uninstall or remove Kaspersky products from their devices when they have been replaced.

Also of note is BIS's rationale for making such a determination and what it may mean for future ICTS investigations and restrictive measures. First, it found that Kaspersky is "subject to the jurisdiction, control, or direction of the Russian government, a foreign adversary." Significant aspects of Kaspersky's business, such as its software design, development, and supply function are conducted in Russia and the legal entity that holds the rights to its IP is organized under the laws of Russia. Because Kaspersky is subject to Russian jurisdiction, it must comply with Russian intelligence and law enforcement efforts, including requests from the Russian Federal Security Service (FSB). While Kaspersky proposed mitigation measures impacting US operations and staffing, BIS concluded that these measures did little to "address the risks associated with Russian government control and direction."

Second, BIS concluded that Kaspersky's software "can be exploited to identify sensitive US person data and make it available to Russian government actors." While the Determination does not disclose specific instances of this occurring, it reasons that, because Kaspersky software operates at the kernel level, it may be misused to inspect data and files on devices running the software. Kaspersky may also modify software on a user's device to reroute the transmission of data collected by the device to its servers in Russia. In addition, the KSN function that is built into the software could further facilitate the "collection of highly sensitive data from the user's device, such as the IP address, physical location, information about the computer's hardware and software, files downloaded, certain websites visited, running applications, and user account names."

Finally, BIS found that Kaspersky's software allows for "the capability and opportunity to install malicious software and strategically withhold critical malware signature updates" that would leave US users vulnerable to threat actors. Again, Kaspersky's proposed mitigations, including implementation of safeguards to prevent malicious code from being introduced on user devices, did not satisfy BIS, because Kaspersky could still provide the information gathered about user devices to enable malicious cyber actors to target those devices.

The action targeting Kaspersky is not, itself, particularly surprising, given that it was purged from federal networks years ago. But this determination reflects an important milestone as BIS's first exercise of authority to prohibit or restrict ICTS transactions with a "foreign adversary" nexus to protect US national security. In this regard, it has broader implications for US persons and entities that may rely on ICTS designed,

developed, produced, or supplied by persons subject to the jurisdiction or control of a "foreign adversary." It foreshadows potential future restrictions on the use of other software products and hardware by the private sector, notably including such products and hardware from China. BIS recently initiated an investigation of connected-vehicle technology, and the Biden Administration previously indicated that it was investigating certain Chinese technology companies under the same authority. By relying on fundamental information about the legal status and jurisdiction of a technology company and the nature of their products and services to conclude that an ICTS transaction poses undue or unacceptable risks, companies facing such investigations may face challenges convincing BIS that any proposed mitigation, beyond possible divestment or offshoring of operations to more friendly countries, will eliminate undue or unacceptable risks.

ENTITY LIST AND SDN DESIGNATIONS

In addition to the Determination, BIS and OFAC took the following additional measures with respect to Kaspersky and its senior leadership:

- *BIS Entity List Designations*. On June 20, in conjunction with its announcement of the ICTS Determination, BIS also announced the imposition of sweeping US export control restrictions on two Russian and one UK Kaspersky entities on the BIS Entity List. The designated entities are AO Kaspersky Lab (Russia), OOO Kaspersky Group (Russia), and Kaspersky Labs Limited (UK). As a result of the designation, no person (whether US or non-US) may without authorization export, re-export, or transfer (in-country) any goods, software, or technology subject to US export controls when any of these entities is a party to the transaction.
- *OFAC Sanctions Designations of Senior Leadership*. On June 21, OFAC sanctioned twelve individual officers and directors of Kaspersky by designating them as Specially Designated Nationals on its SDN List under Executive Order 14024. As a consequence, US Persons may not engage in any transactions or dealings directly or indirectly involving these individuals, their property or property interests. Non-US persons may also be subject to potential secondary sanctions for facilitating significant transactions for or on behalf of these individuals or their close family members.

---

[1] To date, Commerce has defined the following as "foreign adversaries:" China (including Hong Kong), Russia, Cuba, Iran, North Korea, and Nicolas Maduro/the Maduro Regime in Venezuela.

AUTHORS

ASSOCIATE

AARON FUTERMAN

WASHINGTON DC +1 202 263 3161

AFUTERMAN@MAYERBROWN.COM

PARTNER

ADAM S. HICKEY

WASHINGTON DC +1 202 263 3024

NEW YORK

AHICKEY@MAYERBROWN.COM

PARTNER

TAMER A. SOLIMAN

WASHINGTON DC +1 202 263 3292

DUBAI +971 4 375 7160

TSOLIMAN@MAYERBROWN.COM

PARTNER

HOWARD W. WALTZMAN

WASHINGTON DC +1 202 263 3848

HWALTZMAN@MAYERBROWN.COM