FOR IMMEDIATE RELEASE
June 20, 2024
https://bis.gov

BUREAU OF INDUSTRY AND SECURITY
Office of Congressional and Public Affairs
Media Contact: OCPA@bis.doc.gov

Commerce Department Prohibits Russian Kaspersky Software for U.S. Customers

WASHINGTON, D.C. – Today, the Department of Commerce's Bureau of Industry and Security (BIS) announced a Final Determination prohibiting Kaspersky Lab, Inc., the U.S. 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 U.S. 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 and is the first Final Determination issued by BIS's Office of Information and Communications Technology and Services (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. Kaspersky will generally no longer be able to, among other activities, sell its software within the United States or provide updates to software already in use. The full list of prohibited transactions can be found at oicts.bis.gov/kaspersky.

In addition to this action, BIS added three entities—AO Kaspersky Lab and OOO Kaspersky Group (Russia), and Kaspersky Labs Limited (United Kingdom)—to the Entity List for their cooperation with Russian military and intelligence authorities in support of the Russian Government's cyber intelligence objectives.

Today's Final Determination and Entity Listing are the result of a lengthy and thorough investigation, which found that the company's continued operations in the United States presented a national security risk—due to the Russian Government's offensive cyber capabilities and capacity to influence or direct Kaspersky's operations—that could not be addressed through mitigation measures short of a total prohibition.

Individuals and businesses that utilize Kaspersky software are strongly encouraged to expeditiously transition to new vendors to limit exposure of personal or other sensitive data to malign actors due to a potential lack of cybersecurity coverage. Individuals and businesses that continue to use existing Kaspersky products and services will not face legal penalties under the Final Determination. However, any individual or business that continues to use Kaspersky products and services assumes all the cybersecurity and associated risks of doing so.

In order to minimize disruption to U.S. consumers and businesses and to give them time to find suitable alternatives, the Department's determination will allow Kaspersky to continue certain operations in the United States—including providing anti-virus signature updates and codebase updates—until 12:00AM Eastern Daylight Time (EDT) on September 29, 2024.

"The Biden-Harris Administration is committed to a whole-of-government approach to protect our national security and out-innovate our adversaries," said **Secretary of Commerce Gina Raimondo**. "Russia has shown time and again they have the capability and intent to exploit Russian companies, like Kaspersky Lab, to collect and weaponize sensitive U.S. information, and we will continue to use every tool at our disposal to safeguard U.S. national security and the American people. Today's action, our first use of the Commerce Department's ICTS authorities, demonstrates Commerce's role in support of our national defense and shows our adversaries we will not hesitate to act when they use their technology poses a risk to United States and its citizens."

"Whether you are shopping online or sending an email, Americans need to know they can rely on the safety and security of their devices," said **Secretary of Homeland Security Alejandro N. Mayorkas**. "The actions taken today are vital to our national security and will better protect the personal information and privacy of many Americans. We will continue to work with the Department of Commerce, state and local officials, and critical infrastructure operators to protect our nation's most vital systems and assets."

"With today's action, the American cyber ecosystem is safer and more secure than it was yesterday," said **Under Secretary for Industry and Security Alan Estevez**. "We will not hesitate to protect U.S. individuals and businesses from Russia or other malign actors who seek to weaponize technology that is supposed to protect its users."

Kaspersky provides IT security solutions—including tools meant to defend 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.

Today's Final Determination finds ICTS transactions involving such products and services, such as the ability to gather valuable U.S. business information, including intellectual property, and to gather U.S. persons' sensitive data for malicious use by the Russian Government, pose an undue or unacceptable national security risk and therefore prohibits continued transactions involving Kaspersky's products and services.

"The Russian Government has proven that it has the capability and intent to exploit Russian companies like Kaspersky to collect sensitive U.S. personal information and compromise the systems and networks that use these products," said **Elizabeth Cannon, Executive Director of the Office of Information and Communications Technology and Services**. "The Department

of Commerce stands ready to assist U.S. businesses and individual consumers across the country to respond appropriately to today's action."

BIS has determined that Kaspersky poses an undue or unacceptable risk to national security for the following reasons:

- **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 anti-virus software.
- **Access to sensitive U.S. customer information through administrative privileges:** Kaspersky has broad access to, and administrative privileges over, customer information through the provision of cybersecurity and anti-virus software. Kaspersky employees could potentially transfer U.S. 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 U.S. customers' computers or to selectively deny updates, leaving U.S. persons and critical infrastructure vulnerable to malware and exploitation.
- **Third-party integration of Kaspersky products:** Kaspersky software is integrated into third-party products and services through resale of its software, integration of its 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. Third-party transactions such as these create circumstances where the source code for the software is unknown. This increases the likelihood that Kaspersky software could unwittingly be introduced into devices or networks containing highly sensitive U.S. persons data.

Kaspersky is a multinational company with offices in 31 countries, servicing users in over 200 countries and territories. Kaspersky provides cybersecurity and anti-virus products and services to over 400 million users and 270,000 corporate clients globally.

The U.S. Government previously took action against Kaspersky in 2017, when 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 U.S. 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. Today's determination by the Department is the latest U.S. Government action in an ongoing effort to protect U.S. citizens' national security.

The Department is working with the Department of Homeland Security (DHS) and Department of Justice (DOJ) to inform U.S. 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 and ensure a smooth transition for customers.

Additional information about this action and publicly available resources can be found on our website [oicts.bis.gov/kaspersky] 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 online here.

Additional Information:

EO 13873, "Securing the Information and Communications Technology and Services Supply Chain," and its implementing regulation at 15 C.F.R. Part 7 allow 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 U.S. 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 U.S. persons. If the Department determines that an ICTS transaction poses an undue or unacceptable risk, the Department, in consultation with its interagency partners, may prohibit the transaction or impose mitigation measures.

As a consequence of this investigation, Kaspersky is prohibited from conducting or participating in certain ICTS transactions with U.S. persons pursuant to today's Final Determination.

The ICTS program became a mission within BIS in 2022. For more information on the ICTS program, visit oicts.bis.gov.

Additional Background on the Entity List

Additions to the Entity List are made under the authority of the Export Control Reform Act of 2018 and its implementing regulations, the Export Administration Regulations (EAR).

The Entity List (supplement no. 4 to part 744 of the EAR) identifies entities for which there is reasonable cause to believe, based on specific and articulable facts, that the entities—including businesses, research institutions, government and private organizations, individuals, and other types of legal persons—that have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy of the United States. Parties on the Entity List are subject to individual licensing requirements and policies supplemental to those found elsewhere in the EAR.

Entity List additions are determined by the interagency End-User Review Committee (ERC), comprised of the Departments of Commerce (Chair), Defense, State, Energy, and where appropriate, the Treasury, based on specific and articulable facts that the entities have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States.

Additional information on the Entity List is available on BIS's website at: https://www.bis.gov/entity-list.