Billing Code

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

Final Determination: Case No. ICTS-2021-002, Kaspersky Lab, Inc.

Pursuant to the authorities granted in Executive Order ("EO") 13873, "Securing the Information and Communications Technology and Services Supply Chain," the Department of Commerce (the "Department") has reviewed transactions involving cybersecurity and anti-virus software supplied by Kaspersky Lab, Inc. (together with all affiliates, subsidiaries, and parent companies, "Kaspersky") to determine (1) whether those transactions are covered ICTS transactions under 15 CFR 7.103(b); 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, as set out in EO 13873 and 15 CFR part 7.

The Department finds that Kaspersky's provision of cybersecurity and anti-virus software to U.S. 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. Consistent with 15 CFR 7.109(a), the Secretary now issues this Final Determination, which sets forth the Department's decision, based on the risks presented in the Initial Determination and the subsequent responses and mitigation proposals from Kaspersky, as further detailed below.

Background

Consistent with 15 CFR 7.1(b), the Secretary evaluates ICTS transactions under this rule on a case-by-case basis. As outlined in 15 CFR 7.103(a), upon receipt of any information identified in 15 CFR 7.100(a), the Secretary may consider any referral for review of a transaction. In a referral dated August 25, 2021, the Department of Justice ("DOJ") requested the Department review ICTS transactions involving Kaspersky's provision of cybersecurity and anti-virus software and related services to persons subject to the jurisdiction of the United States.

Prior to accepting the referral, the Department determined that the referred transactions were covered ICTS transactions, as identified by EO 13873 and consistent with the Department's regulations at 15 CFR part 7.

First, the Kaspersky transactions meet the following criteria set forth in EO 13873(1)(a)(i):

1, The transactions involve information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. Kaspersky is subject to the jurisdiction of the Russian Federation ("Russia"), a foreign adversary designated by 15 CFR 7.4(a)(5).

Second, the referred transactions meet the following criteria set forth in 15 CFR 7.3(a)(1-4):

1. The transactions are conducted by persons subject to the jurisdiction of the United States. Kaspersky offers cybersecurity and anti-virus software products and services in the United States through Kaspersky Lab, Inc., a Massachusetts corporation.[1]

2. The transactions involve property in which any foreign country or national has an interest. AO Kaspersky Lab, a Russian company,[2] holds the rights to intellectual property used in Kaspersky's cybersecurity and anti-virus software offered to U.S. persons,[3] often in combination with an end-user license agreement.[4] Moreover, Kaspersky Lab, Inc. is owned by Kaspersky Labs Limited, a United Kingdom corporation, which in turn is headquartered in Moscow.[5] In addition, Kaspersky Lab Switzerland GmbH, a subsidiary of Kaspersky Labs Limited, sells product licenses to U.S. end users via the Kaspersky website.[6] And finally, threat-related data received from users of Kaspersky products in North America is processed and stored on Swiss servers.[7]

3. The transactions were initiated, pending, or completed on or after January 19, 2021. Kaspersky has offered, and continues to offer, covered ICTS to U.S. persons on or after January 19, 2021.[8]

4. The transactions involve one or more listed types of ICTS. The transactions involve at least three types of ICTS listed in 15 CFR 7.3. First, the purpose and functionality of Kaspersky's cybersecurity and anti-virus software make them integral to both consumer and enterprise computing services, enabling these products and services to use, process, and/or retain sensitive personal data of U.S. customers under 15 CFR 7.3(a)(4)(iii). Second, Kaspersky supplies its products to customers who operate in sectors designated as critical infrastructure by Presidential Policy Directive 21—Critical Infrastructure Security and Resilience under 15 CFR 7.3(a)(4)(i).[9] Finally, the Department assesses that Kaspersky anti-virus and cybersecurity products meet the criteria set forth in 15 CFR 7.3(a)(4)(iv).

Following the determination that the ICTS transactions identified in the DOJ referral were covered transactions under EO 13873 and 15 CFR part 7, the Department commenced an initial review under 15 CFR 7.103 to determine whether the covered ICTS transactions involving Kaspersky cybersecurity and anti-virus software pose undue or unacceptable risks. Pursuant to its authorities, the Department issued an administrative subpoena to Kaspersky on May 25, 2022. At the request of Kaspersky and its counsel upon receiving the subpoena, the Department met with Kaspersky on July 7, 2022, and again on September 1, 2022.

The Department reviewed all documents and information provided by Kaspersky in response to the subpoenas. The Department also reviewed unclassified information provided from U.S. Government agencies, as well as information obtained from public sources (including information available from commercial data services). The Department assessed the covered ICTS transactions according to the criteria identified in 15 CFR 7.103(c) and (d) and made its preliminary assessment that the transactions pose undue or unacceptable risk. The Department consulted with the appropriate agency heads regarding its preliminary assessment, including the information considered, analysis, and ultimate assessment. Following the interagency consultation, the Department reached its Initial Determination, consistent with 15 CFR 7.105,

which proposed to prohibit certain covered ICTS transactions. Kaspersky was served with the Initial Determination on October 5, 2023.

The Initial Determination provided Kaspersky with an explanation as to why transactions involving Kaspersky cybersecurity and anti-virus software meet the criteria of 15 CFR 7.103(b). The Initial Determination further explained the Department's assessment that ICTS transactions to which Kaspersky is a party pose undue and unacceptable risks, as contemplated by EO 13873 and 15 CFR part 7. Accordingly, the Initial Determination recommended the Department prohibit certain ICTS transactions involving Kaspersky cybersecurity and anti-virus software.

On December 7, 2023, at the request of Kaspersky and its counsel, Kaspersky briefed the Department on its response to the Initial Determination. The Department instructed Kaspersky to condense all relevant information into a written response, pursuant to 15 CFR 7.107, and to provide it no later than January 3, 2024.

On January 3, 2024, Kaspersky submitted its official written response to the Initial Determination, which included Kaspersky's challenges to the basis of the Initial Determination, as well as proposed mitigation measures to address the identified risks. On January 9, 2024, the Department acknowledged receipt of Kaspersky's written response and requested additional information regarding Kaspersky's arguments and proposals. On January 12, 2024, Kaspersky submitted its response to the Department's request for additional information, providing further details regarding its proposed mitigation measures (hereinafter, the January 3 and 12 responses are collectively referred to as the "Written Submission").

In its Written Submission, Kaspersky challenged the Initial Determination under 15 CFR 7.107(a) as lacking a sufficient factual or other basis to justify the proposed prohibition. Kaspersky did not provide any new material information or evidence in support of its arguments that had not already been disclosed and considered in the investigation leading up to the Initial Determination. Kaspersky instead made arguments challenging the basis for the Initial Determination, which are further identified in Appendix A. The Department considered

Kaspersky's arguments and addressed each as reflected in Appendix A. Ultimately, the Department determined that, contrary to Kaspersky's arguments, the proposed prohibition under 15 CFR 7.109(a) is well-supported, as discussed in Appendix A and below. Appendix A, attached, includes a detailed response to Kaspersky about how the Department considered the information and mitigation proposals provided by Kaspersky during the course of this review. As it contains business confidential information, it is protected from public disclosure under 15 CFR 7.102(a).

Risk Determination

The Department reviewed covered ICTS transactions involving Kaspersky cybersecurity and anti-virus software and determined that those transactions pose undue or unacceptable risks, as set out in Section 1(a) of EO 13873 and 15 CFR part 7. At the outset, it is worth noting that regardless of whether Kaspersky's products contribute to greater cybersecurity for its customers, this does not necessarily, in the aggregate, increase national security. The risks to U.S. national security addressed in this Final Determination stem not from whether Kaspersky's products are effective at identifying viruses and other malware, but whether they can be used strategically to cause harm to the United States.

The Department identified the following three aspects of Kaspersky cybersecurity and anti-virus software that contribute to the undue and unacceptable risks posed to the national security of the United States and the security and safety of U.S. persons:

I. *Kaspersky is subject to the jurisdiction, control, or direction of the Russian government, a foreign adversary*.

The Department's regulations at 15 CFR 7.4(a)(5) identify Russia as a "foreign adversary." Russia has demonstrated an intent and capability to sabotage or subvert ICT systems in the United States and exfiltrate sensitive data of U.S. persons for use in espionage, influence, or other malicious activities. Russia's malicious activity is documented in public and open-source information.[10]

Significant aspects of Kaspersky's global business are conducted in Russia, including software design, development, and supply. The legal entity that holds the rights to Kaspersky's intellectual property, AO Kaspersky Lab, is organized under the laws of Russia.[11] Kaspersky's founder, majority owner, and current Chief Executive Officer, Eugene Kaspersky, is a Russian national who resides in Russia.[12] Consequently, Kaspersky is subject to the jurisdiction or direction of the Russian government. This fact was not disputed by the company in its responses.

As an entity subject to Russian jurisdiction, it must comply with any Russian government request for assistance or information. Russian laws compel companies subject to Russian jurisdiction to cooperate with Russian intelligence and law enforcement efforts, to include requests from the Russian Federal Security Service ("FSB").[13] In its responses to the Department's subpoenas and its Written Submission, Kaspersky did not dispute that it is obligated to comply with requests from the FSB. Accordingly, Russia, through its jurisdiction, direction, or control over Kaspersky, could exploit access to sensitive information present on electronic devices that use Kaspersky's cybersecurity and anti-virus software in the United States or install or inject new malware through manipulation of Kaspersky's signature library and source code updates.

In its Written Submission, Kaspersky proposed two mitigation measures to address Russian jurisdiction, control, or direction over its actions. These measures generally proposed changes to Kaspersky's U.S. operations and staffing, but modifying U.S. operations and staffing, without severing U.S. operations' ties with Kaspersky's foreign operations, does little to address the risks associated with Russian government control and direction. The proposed mitigation measures do not impact the technical operations, which allow logical access by foreign employees, including in Russia. As a result, the proposed mitigation measures do little to impair Russia's ability to compel Kaspersky to provide the Russian government access to U.S. customer systems and information. Consequently, as further explained in Appendix A, the Department determined that the proposed mitigation measures are insufficient.

II. *Kaspersky's software can be exploited to identify sensitive U.S. person data and make it available to Russian government actors*.

Through its anti-virus and cybersecurity software, Kaspersky, and certain of its employees, necessarily gain access to sensitive U.S. person data. Kaspersky employs several thousand employees across offices in Russia and other foreign countries to develop and refine the source code for Kaspersky's anti-virus and cybersecurity software, to compile the threat signatures, and manage threat information that ultimately gets sent to end-user devices around the world, including in the United States.[14] Consequently, Kaspersky technical engineers have intimate knowledge of vulnerabilities and backdoors that may exist in the software operating on U.S. person devices, which could allow Kaspersky engineers to exploit those devices. Because cybersecurity and anti-virus software necessarily operates at the kernel level (*i.e.*, the core of the operating system, allowing for full access to all systems on the device), this access may be misused to inspect the data and files stored or transited through the electronic devices that use Kaspersky's cybersecurity and anti-virus software. Additionally, Kaspersky may modify the software on a user's device to reroute the transmission of data collected by the device, which can include personal and proprietary user data, to Kaspersky servers located in Russia, or otherwise accessible from Russia. Exploiting this access would provide the Russian government with vectors to conduct espionage, compromise specific devices or networks, gather U.S. business information (including intellectual property), and access U.S. person sensitive data.

The Department additionally assesses that the Kaspersky Security Network (KSN)[15] function that is built into the software could further facilitate the Russian government's targeted 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. User systems that participate in the KSN send data about users' suspicious files or applications through the KSN for analysis based on certain Kaspersky-identified threat indicators. These threat indicators are proprietary,

can be updated or changed daily, and could be used to scour user data to identify and collect sensitive user information for review by Kaspersky through the KSN.[16]

The integration of Kaspersky software into third-party hardware or software, or any "white labeling" of Kaspersky software, further exacerbates these risks as the user would be less likely to know the true source of the code, increasing the likelihood Kaspersky software could unwittingly be introduced into devices or networks containing highly sensitive U.S. data.

In its Written Submission, Kaspersky denies that the company could purposefully obtain sensitive data on U.S. persons.[17] Kaspersky argues that its operations and employees in Russia can only access data that is not attributable to a specific individual, and/or is used in aggregated statistics.[18] The Department disagrees with that argument. As further described in Appendix A, the data security policies the company has in place are internal policies that can be modified by Kaspersky leaders at will. Additionally, Kaspersky engineers who work on anti-virus or cybersecurity software can circumvent those policies by designing vulnerabilities into the source code. Moreover, while Kaspersky alleges the data retrieved is not attributable to a specific individual, Kaspersky's end-user license agreement standard language identifies various types of data that the software collects, such as unique device identifiers, user registration data, location information and images, and information about the operating system of the device and versions of other software present, which could be used to track devices on networks, websites visited, and user location, and ultimately identify the user in a personal or professional capacity.[19] For certain services provided by Kaspersky, the end-user license agreement clearly identifies a capability to locate a lost device, including functionality that enables the operation of the device's camera.[20]

Kaspersky proposed several technical and operational mitigation measures to address this aspect of the undue or unacceptable risk. These measures have been individually as well as collectively considered and addressed by the Department in Appendix A. None of the measures (either combined or in the aggregate) was assessed to be completely effective in mitigating the

identified risks. Among other things, the proposed measures did not adequately address the technical risks associated with source code vulnerabilities that may exist in the anti-virus and cybersecurity software design process, which largely occurs outside of the United States. Therefore, the Department found that Kaspersky's proposals under this aspect are not sufficient to address the identified risks.

III. *Kaspersky cybersecurity and anti-virus software, developed and supplied from Russia, allows for the capability and opportunity to install malicious software and strategically withhold critical malware signature updates*.

As discussed above, Kaspersky develops and controls access to the technology and code infrastructure for its cybersecurity and anti-virus products and may determine the level of access granted to employees. Kaspersky's software operates at the kernel level, providing company employees the capability to acquire unhindered access to all systems on the device. Consequently, Kaspersky software can enable the Russian government—either directly, or through Kaspersky employees under the direction of the Russian government—to sabotage or subvert the integrity of ICTS in the United States. This could include actions to facilitate the installation of malicious tools on U.S. persons' devices and networks, as well as actions to strategically delay or prevent malware signature updates from reaching certain customers in a timely manner. The delay or denial of signature updates would leave these users vulnerable to malicious actors who could target exploitation of known devices and networks.

In its Written Submission, Kaspersky argued that it has implemented multiple safeguards to prevent malicious code from being introduced to a user's device.[21] These arguments have been considered and are addressed by the Department in greater detail in Appendix A. At a general level, the safeguards identified would not address a fundamental aspect of the risk—namely, that Kaspersky does not have to affirmatively inject malware through its own code. Instead, through its persistent access to devices, Kaspersky can provide information about the devices on which its software operates, to enable malicious cyber actors—whether in the Russian government or

aligned therewith—to gain access to those devices and manipulate settings on the device. Additionally, Kaspersky's global virus scanning operation puts it at the forefront for identifying new vulnerabilities in existing software, providing it with significant non-public information for ways to exploit certain versions of software, as well as a list of devices that run that software. This capability, if leveraged by the Russian government, greatly enhances its ability to conduct cyber espionage and to steal sensitive data.

In its Written Submission, Kaspersky also proposed additional technical and operational mitigation measures to address this aspect of the undue or unacceptable risk.[22] As described in Appendix A, the Department concluded that these measures, when considered both individually and in combination with one another, do not sufficiently address the identified risk. The Department determined they fail largely for the same reasons described above regarding the company's existing safeguards. Specifically, the proposed technical and operational mitigation measures address neither the risks associated with intentional withholding of new threat signatures nor the risks associated with Kaspersky's ability to use its kernel-level access to U.S. user systems for a variety of malign purposes.

Final Determination

Pursuant to 50 U.S.C. 1701 *et seq*., EO 13873, and 15 CFR 7.109, and in light of its assessment of the aforementioned risks, as described above and in further detail in Appendix A, including the consideration and determination of insufficiency of Kaspersky's proposed measures to mitigate the risks identified, the Department hereby issues this Final Determination regarding the following ICTS transactions, as that term is defined under 15 CFR 7.2, with U.S. persons:

1. ICTS transactions involving any cybersecurity product or service designed, developed, manufactured, or supplied, in whole or in part, by Kaspersky, to include those products and services listed in Appendix B;

2. ICTS transactions involving any anti-virus software designed, developed, manufactured, or supplied, in whole or in part, by Kaspersky to include those products and services listed in Appendix B; and

3. ICTS transactions involving 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).

Effective at 12 a.m. EDT on July 20, 2024, in accordance with 15 CFR 7.109(d)(5), Kaspersky, and any of its successors and assignees, is prohibited from entering into any new agreement with U.S. persons involving one or more ICTS transactions identified above.

Effective 12 a.m. EDT on September 29, 2024, in accordance with 15 CFR 7.109(d)(5), Kaspersky, and any of its successors or assignees, shall be prohibited from engaging in the identified ICTS transactions in the United States or with U.S. persons, including (1) providing any anti-virus signature updates and codebase updates associated with the ICTS transactions identified above; and (2) operating KSN in the United States or on any U.S. person's information technology system. Kaspersky may continue to operate the KSN for U.S. persons, as well as provide anti-virus signature updates and codebase updates to current U.S. subscribers and users of cybersecurity and anti-virus products and services as identified in Appendix B, until 12:00 AM EDT on September 29, 2024.

Pursuant to the above determination, effective 12:00 AM EDT on September 29, 2024, any 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 is prohibited in the United States or by U.S. persons.

This Final Determination shall 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.

In accordance with 15 CFR 7.200, any person who violates, attempts to violate, conspires to violate, or causes any knowing violation of this Final Determination prohibiting certain classes of ICTS transactions is subject to civil penalties. In accordance with 15 CFR 7.200, any person who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids and abets in the commission of a violation of this Final Determination prohibiting certain classes of ICTS transactions is subject to criminal penalties.

This document of the Department of Commerce was signed on June 14, 2024, by Gina M. Raimondo, Secretary of Commerce. The document with the original signature and date is maintained by the Department of Commerce. For administrative purposes only, and in compliance with requirements of the Office of the Federal Register, the undersigned Department of Commerce Federal Register Liaison Officer has been authorized to sign and submit the document in electronic format for publication, as an official document of the Department of Commerce. This administrative process in no way alters the legal effect of this document upon publication in the Federal Register.

Signed in Washington, DC, on June 14, 2024.

Beth Grossman,
Federal Register Liaison Officer,
U.S. Department of Commerce.

[FR Doc. 2024-13532 Filed: 6/20/2024 4:15 pm; Publication Date: 6/24/2024]

[1] *Business Entity Summary: Kaspersky Lab, Inc.*, SEC. OF THE COMMONW. OF MASS. CORP. DIV., https://corp.sec.state.ma.us/CorpWeb/CorpSearch/CorpSummary.aspx?sysvalue=dfuXePdZwyoTa04_4VJnwjfqm1XFpXmuQMqvGjYKkM0- (last visited May 29, 2024).
[2] *AO Kaspersky Lab*, Kaspersky Internet Security 2019, KASPERSKY (Aug. 13, 2019), https://support.kaspersky.com/kis/2019/en-US/34744.htm.
[3] *Kaspersky Lab – Global Privacy Policy*, KASPERSKY, https://www.kaspersky.com/global-privacy-policy (last visited May 29, 2024).

[4] *See, e.g.*, KASPERSKY, END USER LICENSE AGREEMENT FOR KASPERSKY VIRUS REMOVAL TOOL (2021), https://support.kaspersky.com/us/kvrt2015/licensing/8530#block3 (last visited May 29, 2024).
[5] *Company Overview*, KASPERSKY, https://usa.kaspersky.com/about/company (last visited May 29, 2024); https://esg.kaspersky.com/report/esg_report_2021-2022_en.pdf (last accessed on May 3, 2024).
[6] *See Kaspersky Endpoint Security for Business*, KASPERSKY, https://usa.kaspersky.com/small-to-medium-business-security/endpoint-protection (last visited May 29, 2024).
[7] *Kaspersky Global Transparency Initiative*, KASPERSKY, https://www.kaspersky.com/transparency-center (last visited May 29, 2024).
[8] *See Complete Security Plans for You & Your Family*, KASPERSKY, https://usa.kaspersky.com/home-security (last visited May 29, 2024).
[9] *See Kaspersky Enterprise Industries*, KASPERSKY, https://www.kaspersky.com/enterprise-security/industries (last visited May 29, 2024).
[10] *See, e.g.*, *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*, U.S. DEP'T OF JUST. OFF. OF PUB. AFF. (Oct. 19, 2020) https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.
[11] *Kaspersky Lab – Global Privacy Policy*, KASPERSKY, https://www.kaspersky.com/global-privacy-policy (last visited May 29, 2024).
[12] *Eugene Kaspersky Bio*, KASPERSKY, https://www.kaspersky.com/about/team/eugene-kaspersky (last visited May 29, 2024); *see also Eugene Kaspersky Profile*, FORBES, https://www.forbes.com/profile/eugene-kaspersky/?sh=4a8a767e34d7 (last visited May 29, 2024).
[13] *See Report of Peter B. Maggs to the Department of Homeland Security* at 4 (Dec. 2, 2017), https://www.internetgovernance.org/wp-content/uploads/12-7-Exhibit-AR-Part-6-Maggs-report.pdf. In addition to complying with Federal Law No. 40-FZ, the Report of Peter B. Maggs explains that companies such as Kaspersky may also be obligated to assist the FSB with operational-investigative activities undertaken in the performance of FSB duties, such as by installing equipment supplied by the FSB for use in obtaining information stored on computers. *Id.* at 8-11 (citing Federal Law No. 144-FZ of August 12, 1995 (as amended), "On Operational-Investigative Activity").
[14] *Company Overview*, KASPERSKY, https://usa.kaspersky.com/about/company (last visited May 29, 2024).
[15] *Kaspersky Security Network (KSN)*, KASPERSKY, https://www.kaspersky.com/ksn (last visited May 29, 2024).
[16] KASPERSKY LAB, KASPERSKY PRIVATE SECURITY NETWORK: REAL-TIME THREAT INTELLIGENCE – INSIDE THE CORPORATE INFRASTRUCTURE (White Paper, 2015), https://media.kaspersky.com/en/business-security/enterprise/KPSN_Whitepaper.pdf.
[17] *Response to and Proposed Measures to Mitigate Risks Identified in Initial Determination, Case No. ICTS-2021-002*, Jan. 3, 2024, at 10 ("January 3rd Response").
[18] January 3rd Response at 10.
[19] AO KASPERSKY LAB, KASPERSKY (APPLICATION FOR ANDROID) END USER LICENSE AGREEMENT (2022), https://products.s.kaspersky-labs.com/homeuser/kisa/11.96.4.9614/english-20230327_161605/3730363534317c44454c7c4e554c4c/eula_basic.html (last visited May 29, 2024).
[20] AO KASPERSKY LAB, KASPERSKY (APPLICATION FOR ANDROID) END USER LICENSE AGREEMENT at Art. 4 (2022), https://products.s.kaspersky-labs.com/homeuser/kisa/11.96.4.9614/english-20230327_161605/3730363534317c44454c7c4e554c4c/eula_basic.html (last visited May 29, 2024).
[21] January 3rd Response at 10.
[22] January 3rd Response at 13-14.