PUBLIC NOTICE

Federal Communications Commission
45 L St., N.E.
Washington, D.C. 20002

News Media Information 202 / 418-0500
Internet: https://www.fcc.gov
TTY: 1-888-835-5322

DA 24-712
Released: July 23, 2024

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU ANNOUNCES UPDATE TO LIST OF COVERED EQUIPMENT AND SERVICES PURSUANT TO SECTION 2 OF THE SECURE NETWORKS ACT

WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233

Pursuant to section 2 of the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act),[1] and sections 1.50002 and 1.50003 of the Commission's rules,[2] the Federal Communications Commission's Public Safety and Homeland Security Bureau (Bureau) announces the addition of cybersecurity and anti-virus software produced or provided by Kaspersky Lab, Inc., together with all affiliates, subsidiaries, and parent companies (Kaspersky), to the list of communications equipment and services (Covered List) that have been determined to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons. The updated Covered List is reproduced in full in the Appendix to this Public Notice and is also found on the Bureau's website at https://www.fcc.gov/supplychain/coveredlist.

Consistent with section 2 of the Secure Networks Act, the Commission adopted rules in the *Supply Chain Second Report and Order* governing the publication and update of the Covered List and tasked the Bureau with publishing and maintaining the Covered List on the Commission's website.[3] The Commission's rules require the Bureau to place on the Covered List any communications equipment or service if a source enumerated in the Secure Networks Act determines that the equipment or service poses an unacceptable risk to the national security of the United States,[4] and if the communications equipment or service is capable of posing an unacceptable risk to the national security of the United States.[5] One of the sources enumerated in the Secure Networks Act is "[a] specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 . . . relating to securing the information

[1] 47 U.S.C. § 1601; *see* Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) (Secure Networks Act).

[2] 47 CFR §§ 1.50002, 1.50003; *see Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14284 (2020) (*Supply Chain Second Report and Order*).

[3] *See Supply Chain Second Report and Order*, 35 FCC Rcd at 14311-25, paras. 57-92; 47 CFR §§ 1.50002 & 1.50003.

[4] Secure Networks Act § 2(b)(1); 47 CFR § 1.50002(b)(1). The Secure Networks Act does not give the Commission discretion to make any updates to the Covered List outside of determinations made by the sources enumerated in section 2(c). *See Supply Chain Second Report and Order*, 35 FCC Rcd at 14324-25, para. 91.

[5] Secure Networks Act § 2(b)(2); 47 CFR § 1.50002(b)(2).

and communications technology and services [(ICTS)] supply chain."[6] The Secure Networks Act and the Commission's rules require the Bureau to monitor the status of determinations in order to keep the Covered List up to date.[7] Today, we update the Covered List based on a specific determination issued by the Department of Commerce.

On June 20, 2024, the Department of Commerce issued a Final Determination that prohibits Kaspersky, and any of its successors or assignees, from engaging in ICTS transactions with U.S. persons involving cybersecurity products or services and anti-virus software designed, developed, manufactured, or supplied, in whole or part, by Kaspersky, including the integration of such software into third-party products or services.[8] In the Final Determination, the Department of Commerce found 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."[9]

The Commission previously updated the Covered List in March 2022 to include the "information security products, solutions, and services" of AO Kaspersky,[10] based on a Binding Operational Directive (BOD) issued by the Department of Homeland Security that required certain federal agencies to remove "Kaspersky-branded products" from federal information systems.[11] Consistent with Commerce's Final Determination, our action today reflects a broader set of equipment and services produced or provided by Kaspersky, including as explained above, commercial hardware or software containing Kaspersky

[6] Secure Networks Act § 2(c)(2); 47 CFR § 1.50002(b)(1)(ii). In 2021, pursuant to Executive Order 13873, the Department of Commerce promulgated rules governing the review of transactions involving ICTS to determine whether such transactions present national security risks. *See* 15 CFR § 7.1 *et seq.*; Executive Order 13873 of May 15, 2019, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689 (May 15, 2019). These rules authorize the Department of Commerce to examine transactions involving ICTS designed, developed, manufactured, or supplied by persons or entities owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. 15 CFR § 7.1. Foreign adversary is a foreign government or foreign non-government person who the Secretary of Commerce has determined to "have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons." 15 CFR § 7.4. Currently, foreign adversary is defined as including the People's Republic of China, Cuba, Iran, North Korea, Russia, and Venezuela. *Id.* If the Department of Commerce determines that the ICTS transactions poses undue or unacceptable risks to the national security of the United States or the security and safety of United States persons, the Department of Commerce may block or restrict the transaction. 15 CFR § 7.1.

[7] 47 U.S.C. § 1601(d)(1)-(2); 47 CFR § 1.50003(a)-(b).

[8] Department of Commerce, Final Determination, Case No. ICTS-2021-002, Kaspersky Lab, Inc., 89 Fed. Reg. 52434 (June 24, 2024) (Final Determination), https://www.federalregister.gov/documents/2024/06/24/2024-13532/final-determination-case-no-icts-2021-002-kaspersky-lab-inc.

[9] *Id.* at 52434.

[10] The DHS Binding Operation Directive referred to Kaspersky as AO Kaspersky, using the formal Russian corporate nomenclature "AO" (Aktsioenernoye Obshchestvo) for Russian stock companies. *See generally* Cameron McKenna, *"Business Structures in Russia,"* CMS Law-Now (Aug. 25, 2004), https://cms-lawnow.com/en/ealerts/2004/08/business-structures-in-russia.

[11] *Public Safety and Homeland Security Bureau Announces Additions to the List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, WC Docket No. 18-89, Public Notice (PSHSB Mar. 25, 2022) (citing and quoting National Protection and Programs Directorate, DHS, *Notification of Issuance of Binding Operational Directive 17-01 and Establishment of Procedures for Responses*, 82 Fed. Reg. 43782, 43783 (Sept. 19, 2017) (BOD), https://www.federalregister.gov/documents/2017/09/19/2017-19838/national-protection-and-programs-directorate-notification-of-issuance-of-binding-operational. The Bureau placed certain Kaspersky-branded products on the Covered List based on DHS's BOD finding that such services pose an unacceptable risk to the national security of the U.S. and U.S. persons. *Id.* at 2.

cybersecurity and anti-virus software.[12]

To request materials in accessible formats (such as Braille, large print, electronic files, or audio format), send an e-mail to: fcc504@fcc.gov, or call the Consumer and Governmental Affairs Bureau at (202) 418-0530.

For further information, please contact Zenji Nakazawa, Associate Bureau Chief, Public Safety and Homeland Security Bureau at 202-418-7949 or Zenji.Nakazawa@fcc.gov.

– FCC –

[12] Final Determination at 52437. The Binding Operational Directive explicitly "d[id] not address Kaspersky code embedded in the products of other companies." BOD at 43783.

APPENDIX

COVERED LIST (Updated July 23, 2024)*†

Covered Equipment or Services*	Date of Inclusion on Covered List
Telecommunications equipment produced or provided by **Huawei Technologies Company**, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Telecommunications equipment produced or provided by **ZTE Corporation**, including telecommunications or video surveillance services provided or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by **Hytera Communications Corporation**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by **Hangzhou Hikvision Digital Technology Company**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced or provided by **Dahua Technology Company**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services produced or provided by such entity or using such equipment.	March 12, 2021
Information security products, solutions, and services supplied, directly or indirectly, by **AO Kaspersky Lab** or any of its predecessors, successors, parents, subsidiaries, or affiliates.	March 25, 2022
International telecommunications services provided by **China Mobile International USA Inc.** subject to section 214 of the Communications Act of 1934.	March 25, 2022
Telecommunications services provided by **China Telecom (Americas) Corp.** subject to section 214 of the Communications Act of 1934.	March 25, 2022
International telecommunications services provided by **Pacific Networks Corp.** and its wholly-owned subsidiary **ComNet (USA) LLC** subject to section 214 of the Communications Act of 1934.	September 20, 2022
International telecommunications services provided by **China Unicom (Americas) Operations Limited** subject to section 214 of the Communications Act of 1934.	September 20, 2022
Cybersecurity and anti-virus software produced or provided by **Kaspersky Lab, Inc.** or any of its successors and assignees.	July 23, 2024

*The inclusion of producers or providers of equipment or services identified on this list should be read to include the subsidiaries and affiliates of such entities.

†Where equipment or services on the list are identified by category, such category should be construed to include only equipment or services capable of the functions outlined in sections 2(b)(2)(A), (B), or (C) of the Secure and Trusted Communications Networks Act of 2019, 47 U.S.C. § 1601(b)(2)(A)-(C).