PUBLIC NOTICE

Federal Communications Commission
45 L St., N.E.
Washington, D.C. 20554

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

DA 22-320
Released: March 25, 2022

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

Pursuant to sections 2(a) and (d) 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 following additions to the list of communications equipment and services (Covered List) that have been determined by the Department of Homeland Security and an executive branch interagency body with appropriate national security expertise to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons.[3] The updated Covered List reproduced in the Appendix to this Public Notice is also found on the Bureau's website at https://www.fcc.gov/supplychain/coveredlist.

The *Supply Chain Second Report and Order* adopted rules governing the maintenance, including updates, of the Covered List and tasked the Bureau with both publishing and maintaining it on the Commission's website in accordance with the Commission's rules.[4] The Commission's rules require[5] the Commission 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

[1] 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] *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*) (adopting 47 CFR §§ 1.50002, 1.50003).

[3] 47 U.S.C. § 1601(d)(1); 47 CFR § 1.50003(a).

[4] *See Supply Chain Second Report and Order*, 35 FCC Rcd at 14311-25, paras. 57-92.

[5] The Commission found that if a determination by an enumerated national security agency, or intergovernmental agency with national security expertise, "indicates that a specific piece of equipment or service poses an unacceptable risk to the national security of the United States and the security and safety of United States persons, the Commission will automatically include this determination on the Covered List." *Supply Chain Second Report and Order*, 35 FCC Rcd at 14382, para. 80. The Commission took this approach "because of the plain language in section 2(b)(2)(C) which lists, among other equipment or service capabilities mandating inclusion on the Covered List, whether the equipment or service poses an unacceptable risk to the national security of the United States or the security and safety of United States persons. If an enumerated source has already performed this analysis as part of its determination, the only action we need take is to incorporate this determination onto the Covered List." *Id.* The Commission, in adopting the rules, interpreted Congress's use of the words "shall place" to mean we have no discretion to disregard determinations from these enumerated sources. *Supply Chain Second Report and Order*, 35 FCC Rcd at 14312, para. 59.

risk to the national security of the United States, and if the communications equipment or service is capable of posing an unacceptable risk to the national security of the United States.[6] Two of those enumerated sources are the Department of Homeland Security[7] and the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, a group of government agencies that assists the FCC in its public interest review of national security and law enforcement concerns that may be raised by foreign participation in the United States telecommunications services sector, which was formerly known informally as Team Telecom.[8]

The Bureau has identified three determinations, one from the Department of Homeland Security and two from Team Telecom, that meet the statutory requirements for additions to the Covered List.

First, a Binding Operational Directive (BOD), issued by the Department of Homeland Security and published in the Federal Register on September 11, 2017, required certain federal agencies to remove "Kaspersky-branded products" from federal information systems.[9] More specifically, the BOD is a compulsory direction to federal, executive branch, departments and agencies for the purposes of safeguarding information and information systems; federal agencies are required to comply with BODs.[10] The BOD states that, in consultation with interagency partners, the Department of Homeland Security "determined that the risks presented by Kaspersky-branded products justify the issuance of this Binding Operational Directive."[11] Based on the required actions by federal agencies in response to the threats identified in the BOD, we interpret the BOD to be a finding from the Department of Homeland Security that Kaspersky-branded products pose an unacceptable risk to the national security of the United States. Further, by requiring federal agencies to remove Kaspersky-branded products we find that the Department of Homeland Security has determined that its products are capable of posing an unacceptable risk to the national security of the United States and its people.[12]

Second, Team Telecom found that China Telecom (Americas) Corp. (China Telecom) services

---

[6] 47 CFR § 1.50002; *see also* 47 U.S.C. § 1601(b)-(c).

[7] 47 CFR § 1.50002; *see also* 47 U.S.C. § 1601(c)(1), (4). The Secure Networks Act defines "appropriate national security agency" as used in section 2(c)(4) to include the Department of Homeland Security. 47 U.S.C. § 1608(2)(A).

[8] *Supply Chain Second Report and Order*, 35 FCC Rcd at 14312, para. 61. The Executive Branch agencies that jointly made the specific determinations that we recognize here are DOJ, DHS, DOD, the Departments of State and Commerce, and USTR. These agencies are collectively referred to as the Executive Branch agencies. These Executive Branch agencies are either Members of or Advisors to the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, which was created pursuant to Executive Order 13913, 85 Fed. Reg. 19643 (Apr. 4, 2020). *See* The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector - Frequently Asked Questions, https://www.justice.gov/nsd/committee-assessment-foreign-participation-united-states-telecommunications-services-sector.

[9] 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.

[10] 44 U.S.C. §§ 3552(b)(1), 3553(b)(2), 3554(a)(1)(B)(ii).

[11] BOD, 82 Fed. Reg. at 43783.

[12] The Department of Homeland Security issued the BOD pursuant to its authority under the Federal Information Security Modernization Act of 2014 (FISMA), Pub. L. No. 113-283, 128 Stat. 3073. FISMA, among other things, vests the Department of Homeland Security, in consultation with the Office of Management and Budget, to administer the implementation of agency information security policies and practices for information systems, which includes assisting agencies and providing certain government-wide protections, such as BODs. 44 U.S.C. § 3553. The BOD identifies some specific Kaspersky-branded products that were known at the time it was published. *See* BOD, 82 Fed. Reg. at 43783.

associated with its section 214 authorizations, and China Telecom's operations as a carrier in the United States pose substantial and unacceptable risks to U.S. national security and law enforcement concerns.[13] Based on Team Telecom's finding that China Telecom's services associated with its section 214 authorizations pose substantial and unacceptable risks to U.S. national security, we find that Team Telecom also determined that those services are capable of otherwise posing an unacceptable risk to the national security of the United States and its people.

Third, Team Telecom found that services associated with China Mobile International USA Inc. (China Mobile)'s application for a certificate of public convenience and necessity under section 214 of the Communications Act raised "substantial and unacceptable national security and law enforcement risks in the current national security environment."[14] Based on Team Telecom's finding that China Mobile's services associated with its application for section 214 services posed substantial and unacceptable risks to U.S. national security, we find that Team Telecom also determined that the services that China Mobile's application sought authority to provide are capable of otherwise posing an unacceptable risk to the national security of the United States and its people.

The inclusion of these services on the Covered List extends both to subsidiaries and affiliates of the named entities.

Consistent with the Secure Networks Act and the Commission's rules, the Bureau will update this list upon becoming aware of any equipment or service that satisfies the criteria established in section 2 of the Secure Networks Act and section 1.50002 of the Commission's rules.

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

– FCC –

[13] *See generally* Executive Branch Recommendation to the Federal Communications Commission to Revoke and Terminate [CTA's] International Section 214 Common Carrier Authorizations, File Nos. ITC-214-20010613-00346, ITC-214- 20020716-00371, ITC-T/C-20070725-00285, at 1 (filed Apr. 9, 2020) (China Telecom Executive Branch Recommendation). (finding the Executive Branch's recommendation "reflects the substantial and unacceptable national security and law enforcement risks associated with China Telecom's continued access to U.S. telecommunications infrastructure pursuant to its international Section 214 authorizations").

[14] *See generally* Executive Branch Recommendation to the Federal Communications Commission to Deny China Mobile International (USA) Inc.'s Application for an International Section 214 Authorization, File No. ITC-214-20110901- 00289 at 1 (filed July 2, 2018) (finding the application "raises substantial and unacceptable national security and law enforcement risks in the current national security environment").

APPENDIX

COVERED LIST (Updated March 25, 2022)*†

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

*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).