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 22-979
Released: September 20, 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, ET Docket No. 21-232, EA Docket No. 21-233

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 Executive Branch interagency bodies 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 risk to the national security of the United States and if the communications equipment or service is

[1] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, § 2(a), (d), 133 Stat. 158, 158-59 (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, 14375-76 (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 14320, 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 it had no discretion to disregard determinations from these enumerated sources. *Supply Chain Second Report and Order*, 35 FCC Rcd at 14312, para. 59.

capable of posing an unacceptable risk to the national security of the United States.[6]

The Bureau has identified two determinations that meet the statutory criteria for additions to the Covered List. Both determinations were reflected in letters submitted to the Commission on behalf of interested parties of the Executive Branch (Executive Branch entities) by the Department of Commerce's National Telecommunications and Information Administration (NTIA)—one letter concerns Pacific Networks Corp. ("PacNet") and its wholly-owned subsidiary ComNet (USA) LLC ("ComNet") (collectively "PacNet/ComNet")),[7] and the other concerns China Unicom (Americas) Operations Limited ("China Unicom").[8] The letters explain how PacNet/ComNet and China Unicom, respectively, are subject to the exploitation, influence and control of the Chinese government, and the national security risks associated with such exploitation, influence, and control.[9] In recent letters to the Commission, the Department of Justice (DoJ), in coordination with and with the concurrence of the Department of Defense (DoD), confirms that the Executive Branch's views in the PacNet/ComNet Executive Branch Letter and the CUA Executive Branch Letter, respectively, reflect a determination that the international section 214 services provided by PacNet/ComNet and China Unicom involve communications services that pose "an unacceptable risk to the national security of the United States or the security and safety of United States persons" under section 2 of the Secure Networks Act—thus requiring the addition of these services to the Covered List.[10] Accordingly, by this Public Notice, we update the Covered List.

With respect to PacNet/ComNet, the Executive Branch entities found that the Government of the People's Republic of China's (PRC) majority ownership and control of PacNet and its wholly-owned subsidiary ComNet through parent company CITIC Group Corporation, combined with Chinese intelligence and cybersecurity laws, raise concerns that PacNet/ComNet will be forced to comply with Chinese government requests for communications intercepts, without the ability to challenge such requests.[11] The Executive Branch entities also found that PacNet/ComNet's interconnections to U.S. telecommunications networks and customers present opportunity for exploitation by the Chinese government to conduct or to increase economic espionage and collect intelligence against the United States, or otherwise provide a strategic capability to target, collect, alter, block, and re-route network traffic.[12] Additionally, based on the Executive Branch entities' finding that no further mitigation

---

[6] 47 CFR § 1.50002; *see also* 47 U.S.C. §§ 1601(b)(1), 1601(b)(2)(C), 1601(c).

[7] Letter from Kathy Smith, Chief Counsel, National Telecommunications and Information Administration, U.S. Department of Commerce, to Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau at 1 (Nov. 16, 2020) (on file in GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199) (PacNet/ComNet Executive Branch Letter). The interested Executive Branch entities include the Department of Justice, Department of Homeland Security, Department of Defense, Department of Commerce, Department of the Treasury, Department of State, Office of Management and Budget, Office of the U.S. Trade Representative, General Services Administration, and Council of Economic Advisers. *See* PacNet/ComNet Executive Branch Letter at 1 n.3.

[8] Letter from Kathy Smith, Chief Counsel, National Telecommunications and Information Administration, U.S. Department of Commerce, to Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau at 1 (Nov. 16, 2020) (on file in GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427) (CUA Executive Branch Letter).

[9] *See* PacNet/ComNet Executive Branch Letter; CUA Executive Branch Letter.

[10] Letter from Lee Licata, Deputy Section Chief for Telecom and Supply Chain, Foreign Investment Review Section, National Security Division, U.S. Department of Justice, to Marlene H. Dortch, Secretary, Federal Communications Commission (Sept. 15, 2022) (on file in WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233). In its letters, DoJ also notes that the PacNet/ComNet and China Unicom Executive Branch Letters represented the view of DoD, which qualifies as an "appropriate national security agency" authorized to make determinations pursuant to section 2 of the Secure Networks Act. *Id.* at 2.

[11] PacNet/ComNet Executive Branch Letter at 6.

[12] PacNet/ComNet Executive Branch Letter at 10.

measures by PacNet/ComNet would fully eliminate the risks to American law enforcement and national security,[13] the Executive Branch entities have determined that services provided by PacNet/ComNet pose an unacceptable risk to the national security of the United States and its people.

With respect to China Unicom, the Executive Branch entities found that the United States national security environment, including increased concern about malicious cyber activities taken at the direction of the Government of the PRC, has changed significantly since 2002, when the Commission certified the international section 214 authorization of China Unicom to provide international common carrier services;[14] that China Unicom's status as a wholly-owned subsidiary of a PRC state-owned enterprise firmly places it under the exploitation, control, and influence of the Chinese government;[15] that China Unicom has continuing and ongoing commercial relationships with Chinese entities accused of engaging in activities contrary to American national security and economic interests;[16] and that China Unicom's American operations provide opportunity to facilitate Chinese cyber activities including economic espionage, disruption and misrouting of American communications traffic, and access to U.S. records and other sensitive data.[17] Accordingly, based on these findings, the Executive Branch entities have determined that services provided by China Unicom associated with its international section 214 authorization pose a substantial and unacceptable risks 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] PacNet/ComNet Executive Branch Letter at 10-11.

[14] CUA Executive Branch Letter at 2, 2-6.

[15] CUA Executive Branch Letter at 2, 6-11.

[16] CUA Executive Branch Letter at 2-9.

[17] CUA Executive Branch Letter at 2, 34-35.

APPENDIX

COVERED LIST (Updated September 20, 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
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

*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).