PUBLIC NOTICE

Federal Communications Commission
45 L Street NE
Washington, DC 20554

News Media Information 202-418-0500
Internet: www.fcc.gov

DA 25-418
Released: May 23, 2025

THE PUBLIC SAFETY AND HOMELAND SECURITY BUREAU AND THE OFFICE OF ENGINEERING AND TECHNOLOGY SEEK PUBLIC INPUT ON COMMERCE DEPARTMENT DETERMINATION REGARDING CERTAIN CONNECTED VEHICLE TECHNOLOGIES

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

Input Due: June 9, 2025

As detailed below, on January 16, 2025, the Commerce Department's Bureau of Industry and Security (BIS) determined, pursuant to Executive Order No. 13873 (2019),[1] that the provision of certain connected vehicle hardware or software by certain Chinese- or Russian-controlled entities poses an unacceptable risk to U.S. national security and the safety and security of U.S. persons.[2] BIS made this determination in a final rule restricting certain transactions involving such hardware or software because of this unacceptable risk.[3] The final rule delayed certain of the restrictions by adopting specific exemptions.[4]

Section 2 of the Secure and Trusted Communications Networks Act of 2019[5] (Secure Networks Act) requires the Commission to publicize and update 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. Pursuant to the Commission's rules, the Public Safety and Homeland Security Bureau (PSHSB) monitors determinations made by certain federal entities enumerated in the Secure Networks Act and updates the Covered List accordingly.[6] One of those sources is "[a] specific determination made by the Department of Commerce (Commerce) pursuant to Executive Order No. 13873."[7]

The FCC's PSHSB and Office of Engineering and Technology (OET) therefore request input on whether the Covered List should be updated to include certain communications equipment and services,[8]

---

[1] Executive Order 13873 of May 15, 2019, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689 (May 15, 2019) (Executive Order 13873).

[2] *See generally* Department of Commerce, Bureau of Industry and Security, Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 90 Fed. Reg. 5360 (Jan. 16, 2025) (*BIS Connected Vehicles*); 15 CFR § 791.300.

[3] *Id*.

[4] *Id*. § 791.308. The lengths of the exemptions vary depending on the type of transaction and can be set in terms of vehicle model year (*i.e.*, prior to model year 2027 or model year 2030) or date of importation (*i.e.,* prior to January 1, 2029).

[5] 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).

[6] Secure Networks Act § 2(b)(1); 47 CFR § 1.50002(b)(1).

[7] Secure Networks Act § 2(c)(2); 47 CFR § 1.50002(b)(1)(ii).

[8] *See* https://www.fcc.gov/supplychain/coveredlist (last visited Apr. 23, 2025).

on the basis of this recent Commerce Department determination relating to connected vehicles.

We are not required to provide the opportunity for public input on updates to the Covered List under the Commission's rules,[9] and we have not done so in the past.[10] However, because this would be the first addition that does not include the names of specific entities, we believe that offering an opportunity for public input will help promote transparency and good governance. We are limiting this public input period to 15 days, given the finding that these communications equipment and services pose unacceptable risks to national security.

Update to the Covered List:

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 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, and tasked PSHSB with publishing and maintaining the Covered List on the Commission's website.[11] The Commission's rules require PSHSB 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,[12] and if the communications equipment or service is capable of posing an unacceptable risk to the national security of the United States.[13] One of the sources enumerated in the Secure Networks Act is "[a] specific determination made by the Department of Commerce (Commerce) pursuant to Executive Order No. 13873 . . . relating to securing the information and communications technology and services [(ICTS)] supply chain."[14] The Secure Networks Act and the Commission's rules require PSHSB to monitor the

[9] Secure Networks Act § 2(d)(1)-(2); 47 CFR § 1.50003(a)-(b).

[10] *See, e.g.*, *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, Public Notice, 39 FCC Rcd 8395 (2024) (*Kaspersky Public Notice*); *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, Public Notice, 37 FCC Rcd 10735 (2022).

[11] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Second Report and Order, 35 FCC Rcd 14284, 14311-25, paras. 57-92 (2020) (*Supply Chain Second Report and Order*); 47 CFR §§ 1.50002, 1.50003. The potential updated Covered List is reproduced in full in the Appendix to this Public Notice; the current Covered List can be found on PSHSB's website at https://www.fcc.gov/supplychain/coveredlist.

[12] 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.

[13] Secure Networks Act § 2(b)(2)(C); 47 CFR § 1.50002(b)(2)(iii). The Commission has decided that, when the other agency's determination "covers a specific piece of equipment or service and the agency has indicated that such equipment or service poses a national security risk, we are obligated to include it on the Covered List, particularly because one of the three capabilities that warrant inclusion on the list is whether the equipment or service is capable of 'otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons.'" *Supply Chain Second Report and Order*, 35 FCC Rcd at 14321, para. 81.

[14] 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 § 791.1 *et seq.*; Executive Order 13873. 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 § 791.1. A 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

(continued….)

status of determinations in order to keep the Covered List up to date.[15]

On January 16, 2025, Commerce published a final rule in the Federal Register that prohibits transactions involving certain connected vehicles and related software and hardware designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the People's Republic of China, including the Hong Kong Special Administrative Region and the Macau Special Administrative Region, (PRC); or the Russian Federation (Russia).[16] In the final rule, Commerce made a determination that the provision of completed connected vehicles, as well as the provision of automated driving systems (ADS), covered software, and vehicle connectivity systems (VCS) hardware, by PRC or Russian companies pose an unacceptable risk to the safety and security of U.S. persons.[17] Commerce based this determination on numerous findings over a years-long process, including the finding that the PRC and Russia "have adopted political, legal, and regulatory regimes that enable their governments to exercise direct and indirect ownership, control, or influence over entities in the connected vehicle supply chain."[18] Such control over these entities and the ability to access connected vehicles through their components by the PRC and Russia "could enable those foreign adversaries to (1) exfiltrate sensitive data collected by connected vehicles and (2) allow remote access and manipulation of connected vehicles driven by U.S. persons."[19] To address these national security risks, Commerce adopted rules prohibiting transactions involving certain hardware and software related to connected vehicles.[20]

We seek public input on whether to update the Covered List, pursuant to section 2 of the Secure Networks Act and our rules,[21] and if so, whether to do so at this time. Although the final rule delays some of the transaction restrictions by several years,[22] the Commerce Department made a specific determination about unacceptable risks to national security that exist at present.[23] Because the Secure Networks Act requires that the FCC update the Covered List in response to specific determinations, rather than regulations, we seek public input on the significance, if any, of the delays in some of the Commerce Department rules.

In determining the specific communications equipment or services, if any, we should add to the Covered List, we note the Commerce Department's definitions of "automated driving system," "completed connected vehicle," "covered software," "vehicle connectivity system," "VCS hardware," and "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary,"[24] as

persons." 15 CFR § 791.4. 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 pose 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 § 791.1.

[15] Secure Networks Act § 2(d)(1)-(2); 47 CFR § 1.50003(a)-(b).

[16] *See generally BIS Connected Vehicles*.

[17] 15 CFR § 791.300 ("The inclusion in connected vehicles of certain ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of certain foreign adversaries poses undue or unacceptable risks to U.S. national security."). *See also BIS Connected Vehicles*, 90 Fed. Reg. at 5363-71 (making several other similar specific determinations as to "undue or unacceptable risks").

[18] *Id.*, 90 Fed. Reg. at 5366.

[19] *Id.*, 90 Fed. Reg. at 5361.

[20] *See* 15 CFR pt. 791 subpart D.

[21] Secure Networks Act § 2(b)(1); 47 CFR § 1.50002(b)(1).

[22] *Id*. § 791.308.

[23] *Id*. § 791.300; *BIS Connected Vehicles*, 90 Fed. Reg. at 5363-71.

[24] 15 CFR § 791.301.

well as the examples Commerce provides in interpreting these definitions.[25] Specifically, Commerce Department's determination appears to indicate that PSHSB should add the following narrow class of equipment and services to the Covered List:

(1) automated driving systems (ADS) and completed connected vehicles designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the People's Republic of China, including the Hong Kong Special Administrative Region and the Macau Special Administrative Region, (PRC), or the Russian Federation (Russia); and

(2) vehicle connectivity systems (VCS) hardware designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia and intended to be included within a completed connected vehicle in the United States; or VCS hardware with integrated covered software[26] designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.

We seek public input on whether this is a correct implementation of the Commerce Department determination.

Under the Commission's existing rules in section 2.903(a), once added to the Covered List, "covered" equipment is prohibited from receiving new equipment authorizations.[27] Moreover, pursuant to section 2.911 of the Commission's rules, all applicants seeking equipment authorization from the Commission must certify that the equipment is not prohibited from receiving an equipment authorization by virtue of being "covered equipment."[28] By so certifying, the applicant would be certifying that the equipment does not qualify as equipment listed in this Notice as "covered." We tentatively assess that equipment and services listed in Update (1) would not be subject to the equipment authorization process, because completed connected vehicles are generally not radiofrequency devices for which FCC authorization is sought, nor are the collective "hardware and software" systems that make up ADS.[29] In other words, completed connected vehicles and ADS would not be directly subject to any Covered List prohibitions. We seek public input on our assessment.

By contrast, Update (2), if incorporated into the Covered List, would appear to include equipment subject to the equipment authorization process, because VCS hardware generally would require Commission equipment authorization. Any applicant seeking equipment authorization for VCS hardware must, per section 2.911 of the Commission's rules, certify that the equipment is not prohibited from receiving an equipment authorization by virtue of being "covered equipment." In doing so, the applicant would, if Update (2) is made, be affirming that the equipment was not "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia and intended to be included within a completed connected vehicle in the United States," nor does it contain "integrated covered software designed, developed, manufactured, or supplied

[25] *BIS Connected Vehicles*.

[26] The term "covered software," as used here, has the meaning set out in Commerce's rules. *See* 15 CFR § 791.301 (defining "covered software as the "software-based components, including application, middleware, and system software, in which there is a foreign interest, executed by the primary processing unit or units of an item that directly enables the function of Vehicle Connectivity Systems or Automated Driving Systems at the vehicle level," and also clarifying what is not included in the definition of "covered software").

This is to be distinguished from a statement that certain "software" is "covered" because included on the Covered List. *See Kaspersky Public Notice*, 39 FCC Rcd at 8398 ("Cybersecurity and anti-virus software produced or provided by Kaspersky Lab, Inc. or any of its successors and assignees.").

[27] 47 CFR § 2.903(a).

[28] 47 CFR § 2.911(d)(5)(i).

[29] 15 CFR § 791.301.

by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia." The language "persons owned by, controlled by, or subject to the jurisdiction or direction of" gets its meaning from the Commerce Department's definition of "persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" and the examples included in its decision.[30] We seek public input on whether this is the best implementation of the Commerce Department determination.

It would appear that the Commerce Department defined "VCS hardware" broadly,[31] including some equipment that is *not* "intended for inclusion in a completed connected vehicle." The equipment authorization prohibitions that would result from this Update would apply to a narrower class of equipment. Under this potential update, VCS hardware that is not intended for a vehicle would not be "covered" equipment and would still receive authorization. We recognize that telecommunications certification bodies (TCBs) and test labs may face challenges discerning whether any given VCS hardware is "intended" for inclusion in a completed connected vehicle, especially given that previous updates to the Covered List have not involved an "intent" standard. If this update is incorporated into the Covered List, we believe that VCS hardware that satisfies one or more of the following elements would be among the VCS hardware equipment "intended to be included within a completed connected vehicle in the United States":

- Is a telematics control unit.[32]
- Contains integrated covered software.[33]
- Uses spectrum in the 5.895-5.925 GHz band.[34]

---

[30] 15 CFR § 791.301 ("(1) Any person, wherever located, who acts as an agent, representative, or employee, or any person who acts in any other capacity at the order, request, or under the direction or control, of a foreign adversary or of a person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary; (2) Any person, wherever located, who is a citizen or resident of a foreign adversary or a country controlled by a foreign adversary, and is not a United States citizen or permanent resident of the United States; (3) Any corporation, partnership, association, or other organization with a principal place of business in, headquartered in, incorporated in, or otherwise organized under the laws of a foreign adversary or a country controlled by a foreign adversary; or (4) Any corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by a foreign adversary, to include circumstances in which any person identified in paragraphs (a) through (c) possesses the power, direct or indirect, whether or not exercised, through the ownership of a majority or a dominant minority of the total outstanding voting interest in an entity, board representation, proxy voting, a special share, contractual arrangements, formal or informal arrangements to act in concert, or other means, to determine, direct, or decide important matters affecting an entity."); *BIS Connected Vehicles*, 90 Fed. Reg. at 5384-86 (providing examples).

One example of particular relevance to the Commission is Example 26: "Company A is a publicly listed U.S. corporate entity. Company A has a wholly owned subsidiary, Company B, that is organized under the laws of the PRC or Russia and manufactures goods in the PRC or Russia. Because Company B is organized under the laws of the PRC or Russia, Company B would be subject to the jurisdiction of the PRC or Russia. However, Company A is not subject to the jurisdiction of the PRC or Russia." *Id*. at 5385. Therefore, a U.S. company that has a subsidiary organized under PRC laws would not itself be deemed "subject to the jurisdiction of the PRC." *Id*.

[31] 15 CFR § 791.301.

[32] *BIS Connected Vehicles*, 90 Fed. Reg. at 5364, 5392 (explaining that, as the "primary automotive VCS component," the telematics control unit is the "primary interface between the internal network and external communication channels" and that it collects "information about a driver's location, speed, voice patterns, battery state of charge, or other vehicle diagnostic and operation information" from a "vast array of sensors" and then "converts that data into a format that can be transmitted to systems outside the vehicle and then enables that transmission").

[33] 15 CFR § 791.301.

[34] The 5.9 GHz band is primarily used for Intelligent Transportation System (ITS) technologies that provide services for different modes of transport and traffic management, including vehicle-to-everything (V2X) communications, with the spectrum allocated for specific protocols including Dedicated Short-Range Communications (DSRC) and (continued….)

We seek public input as to whether including VCS hardware that satisfies any of these elements correctly implements Commerce's determination that such hardware be "intended to be included within a completed connected vehicle." Are there more effective means of discerning the relevant intent for purposes of Commerce's determination?

Section 2.903(b) of the Commission's rules requires that each "entity named on the Covered List as producing covered communications equipment" must provide to the Commission information regarding its subsidiaries and affiliates.[35] Because our proposed actions would add to the Covered List certain types of equipment, rather than equipment produced or provided by specific named entities, PSHSB's proposed updates would not result in any entity being an "entity named on the Covered List" for purposes of section 2.903(b). Therefore, under that reading, no person would be required to provide such information as a result of this Update.

Certain of the Commission's rules apply to each "entity identified on the Covered List." For instance, section 2.906(d) of the Commission's rules prohibits entities "identified on the Covered List" from obtaining equipment authorization through the Commission's Supplier's Declaration of Conformity (SDoC) process.[36] Instead, they must seek authorization by an application required under section 2.911 of the rules, including the provision of the certification as to whether the applicant is an "entity identified on the Covered List."[37] In addition, the rules governing certification apply to any equipment produced by entities "identified on the Covered List," even if the equipment otherwise qualifies as an "exempted device" under section 15.103 of our rules.[38] Finally, entities "identified" on the Covered List and their equipment are subject to certain restrictions under the Commission's recently-adopted U.S. Cyber Trust Mark program.[39]

For purposes of the potential additions to the Covered List discussed here, implementing the Commerce determination appears to require treating "persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia" as being entities "identified on the Covered List" *only* if the person actually designs, develops, manufactures, or supplies completed connected vehicles, ADS, covered software, or VCS hardware.[40] Accordingly, such an applicant would certify that it is "identified on the Covered List" pursuant to section 2.911(d)(5)(ii), and equipment produced by such persons would not be eligible for authorization through the SDoC process; such equipment would be subject to the rules governing certification. Such equipment also would be ineligible for exempted device treatment under section 15.103 and subject to the restrictions in the U.S. Cyber Trust Mark program.[41]

We seek input on whether implementing the Commerce determination, in the alternative, might require that *all* persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia attest that they are "identified on the Covered List" pursuant to section 2.911(d)(5)(ii) and be excluded from SDoC and the section 15.103 exemptions. Alternatively, we seek public input on whether the sections of our rules referring to entities "identified" on the Covered List are inapplicable when

---

cellular V2X (C-V2X). *See Use of the 5.850-5.925 GHz Band*, ET Docket No. 19-138, Second Report and Order, FCC 24-123 (2024) (adopting rules to address the transition of 5.9 GHz ITS operations from DSRC to C-V2X).

[35] 47 CFR § 2.903(b).

[36] 47 CFR §§ 2.906(d), 2.907(c).

[37] 47 CFR § 2.911(d)(5)(ii).

[38] 47 CFR § 15.103.

[39] 47 CFR §§ 8.204(c), 8.208(c)(2), 8.220(c)(7).

[40] For these purposes, we consider "persons" to include natural persons or individuals as well as corporations and associations existing under or authorized by the laws of either the United States, the laws of any of the Territories, the laws of any state, or the laws of any foreign country. *See* 15 CFR § 791.301.

[41] 47 CFR §§ 15.103(j), 8.204(c), 8.208(c)(2), 8.220(c)(7).

applied to sections of the Covered List that do not name entities.[42]

Finally, we note that pursuant to sections 0.191 and 0.31(i) of the Commission's rules, Commission staff will provide guidance to TCBs, test labs, and equipment authorization applicants on the impact of any updates adopted.

Procedural Matters

Interested parties may file comments on or before the dates indicated on the first page of this document. Comments may be filed using the FCC's Electronic Comment Filing System (ECFS).

- Commenting parties may file comments in response to this Notice in WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233.
- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: https://www.fcc.gov/ecfs/.
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.
    - ☐ Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the FCC's Secretary, Office of the Secretary, Federal Communications Commission.
    - ☐ All hand-delivered or messenger-delivered paper filings for the FCC's Secretary must be delivered to FCC Headquarters at 45 L St., N.E., Washington, DC 20002. The filing hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
    - ☐ Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
    - ☐ U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L St., N.E., Washington, DC 20002, Washington, DC 20554.

People with Disabilities: To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer and Governmental Affairs Bureau at (202) 418-0530 (voice), (202) 418-0432 (tty).

This *Public Notice* shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's ex parte rules. Persons making ex parte presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation. Persons making oral ex parte presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the ex parte presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda, or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during ex parte meetings are deemed to be written ex parte presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission

[42] *See* 47 CFR § 2.906(d); 2.907(c), 2.911(d)(5)(ii); 2.929(b)(3), (c)(2), (d)(1)(ii); 2.932(e)(2); 2.938(b)(2); 2.1033(b)(3), (c)(3); 2.1043(b)(2)(i)(C), (b)(3)(i)(C); 15.103(j).

has made available a method of electronic filing, written ex parte presentations and memoranda summarizing oral ex parte presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's ex parte rules.

For further information, please contact Michael Connelly, Deputy Chief, Policy and Legal Affairs, Operations and Emergency Management Division, Public Safety and Homeland Security Bureau, at 202-418-0132 or Michael.Connelly@fcc.gov and Jamie Coleman, Associate Chief, Office of Engineering and Technology, at 202-418-2705 or Jamie.Coleman@fcc.gov.

– FCC –

APPENDIX

COVERED LIST (Updated MONTH DAY, 2025)*†

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, including equipment with integrated Kaspersky Lab, Inc. (or any of its successors and assignees) cybersecurity or anti-virus software.	July 23, 2024

Automated driving systems and completed connected vehicles designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the People's Republic of China, including the Hong Kong Special Administrative Region and the Macau Special Administrative Region, (PRC), or the Russian Federation (Russia). Vehicle connectivity systems (VCS) hardware designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia and intended to be included within a completed connected vehicle in the United States; or VCS hardware with integrated covered software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of the PRC or Russia.**	[Month] [XX], 2025

*The inclusion of producers or providers of equipment or services named 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).

** This entry on the Covered List relies on the definitions set out in Department of Commerce regulations. *See* 15 CFR § 791.301 (providing definitions of "automated driving system," "completed connected vehicle," "covered software," "vehicle connectivity system," "VCS hardware," and "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary").