I

118TH CONGRESS
2D SESSION

H. R. 8741

To establish the Office of Information and Communications Technology and Services within the Bureau of Industry and Security of the Department of Commerce, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 13, 2024

Ms. SLOTKIN introduced the following bill; which was referred to the Committee on Foreign Affairs, and in addition to the Permanent Select Committee on Intelligence, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To establish the Office of Information and Communications Technology and Services within the Bureau of Industry and Security of the Department of Commerce, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Connected Vehicle National Security Review Act''.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

SEC. 2. THE OFFICE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES.

(a) ESTABLISHMENT.—There is established within the Bureau of Industry and Security of the Department of Commerce an Office of Information and Communications Technology and Services (in this section, referred to as the ''Office'').

(b) EXECUTIVE DIRECTOR.—The head of the Office shall be an Executive Director who reports to the Under Secretary for Industry and Security and shall be designated by the Secretary.

(c) CONTINUATION IN OFFICE OF THE EXECUTIVE DIRECTOR.—An individual serving as the Executive Director before the date of the enactment of this Act may serve as the Executive Director on and after that date without the need for designation under subsection (b).

(d) DUTIES.—The Office shall—

(1) identify and prevent through mitigation or prohibition the undue or unacceptable risk posed by certain ICTS transactions; and

(2) educate industry and other partners on relevant risks and communicate decisions.

(e) SPECIAL HIRING AUTHORITY.—The Executive Director may appoint, without regard to the provisions of sections 3309 through 3318 of title 5, United States Code, candidates directly to positions in the competitive service (as defined in section 2102 of that title).

SEC. 3. TRANSACTION REVIEW PROCESS.

(a) ICTS TRANSACTION REVIEW PROCESS.—The Secretary, acting through the Office of Information and Communications Technology and Services, shall review ICTS transactions according to the following procedures:

(1) REVIEW.—The Secretary may review any ICTS transaction that the Secretary suspects poses an undue or unacceptable risk.

(2) INVESTIGATIVE AUTHORITY.—In reviewing an ICTS transaction described in paragraph (1) the Secretary may do the following:

(A) Require any person subject to the jurisdiction of the United States to furnish under oath, in the form of a report or otherwise, at any time as may be required by the Secretary,

complete information relative to any such transaction.

(B) Require that any such report take a particular form as directed in a request, regulation, or other guidance provided by the Secretary, which may be required before, during, or after any such transaction.

(C) Through any agency, conduct investigations, hold hearings, administer oaths, examine witnesses, receive evidence, take depositions, and require by subpoena the attendance and testimony of witnesses and the production of any book, contract, letter, paper, and other hard copy or document relating to any matter under investigation, regardless of whether any such report has been required or filed.

(b) MITIGATION OF RISK.—

(1) IN GENERAL.—If the Secretary finds that a covered ICTS transaction poses an undue or unacceptable risk under subsection (a), the Secretary shall mitigate the undue or unacceptable risk described in paragraph (2) or prohibit such transaction.

(2) MITIGATION OF RISK AUTHORITY.—The Secretary may choose to mitigate any undue or un-

acceptable risk posed by a covered ICTS transaction reviewed under subsection (a). To mitigate the undue or unacceptable risk, the Secretary may do any of the following with regard to any party to a covered ICTS transaction:

(A) Negotiate, enter into or impose, and enforce any agreement or condition with any such party.

(B) Require adherence to certain cybersecurity standards and other mitigation requirements determined to be necessary by the Secretary.

(C) Require the exclusion (in whole or in part) of certain components, including physical parts or hardware, software, digital services, and digital components, of any ICTS or any sub-component of ICTS from any such transaction.

(D) Anything else the Secretary determines to be appropriate or necessary to mitigate the undue or unacceptable risks.

(3) PROHIBITION OF TRANSACTION.—If the Secretary determines that the undue or unacceptable risk posed by a covered ICTS transaction cannot be

effectively mitigated for any reason as determined by the Secretary, the Secretary—

(A) may prohibit the covered ICTS transaction;

(B) shall notify any party subject to the covered ICTS transaction review of the prohibition; and

(C) may publish any such prohibition in the Federal Register.

SEC. 4. REGULATING PERSON OR JURISDICTION OF CONCERN-CONNECTED COVERED ICTS TRANSACTIONS.

(a) AUTHORIZATION TO ISSUE RULES FOR CERTAIN CLASSES OF COVERED ICTS TRANSACTIONS.—The Secretary may determine that, for certain classes of covered ICTS transactions, an ICTS transaction review described under section 3 may not effectively address undue or unacceptable risks and may promulgate regulations that do the following:

(1) Identify particular covered ICTS transactions and person or jurisdiction of concern which warrant particular scrutiny for undue or unacceptable risk.

(2) Establish mitigation measures to address undue or unacceptable risk, to include prohibitions

related to entities of concern or for classes of covered ICTS transactions.

(3) Establish criteria by which particular covered ICTS transactions or particular classes of participants in the covered ICTS transaction supply chain may be recognized as categorically included in or as categorically excluded from mitigation measures or prohibitions.

(4) Establish particular classes of covered ICTS transactions or parties to transactions that must abide by certain prohibitions or mitigation measures.

(5) Establish procedures to authorize or license transactions otherwise prohibited pursuant to a regulation promulgated under this section.

(6) Any other rule the Secretary determines to be appropriate.

(b) OTHER REVIEW BY SECRETARY PERMITTED.—The promulgation of any regulation under subsection (a) does not preclude the Secretary from initiating a review of any covered ICTS transaction, including a covered ICTS transaction that belongs to an identified category under this section.

SEC. 5. RISK ASSESSMENT.

(a) DNI RISK ASSESSMENT.—Not later than 180 days after the date of the enactment of this Act, and annu-

ally thereafter, the Director of National Intelligence shall submit to the Secretary a risk assessment that relates to threats posed by persons or jurisdictions of concern to the United States by the supply chain of covered ICTS transactions that—

(1) includes specific criteria to evaluate any undue or unacceptable risk to the national security of the United States; and

(2) identifies any person or jurisdiction of concern, participants in such supply chain, and covered ICTS transactions or classes of covered ICTS transactions posing the highest risks to the national security of the United States.

(b) SUBMISSION OF RISK ASSESSMENT.—Not later than 90 days after the date on which the risk assessment is submitted to the Secretary, the Director of National Intelligence shall submit the risk assessment to the relevant congressional committees in unclassified format.

(c) CLASSIFIED ANNEX.—The risk assessment submitted under subsection (b)—

(1) may include a classified annex; and

(2) shall only include specific participants in such supply chain that pose risk to the national security of the United States in the classified annex.

SEC. 6. OTHER AUTHORITIES.

(a) REGULATIONS.—Any regulation the Secretary promulgated under Executive Order 13873 (84 Fed. Reg. 22689; relating to securing the information and communications technology and services supply chain) and Executive Order 14034 (86 Fed. Reg. 31423; relating to protecting Americans' sensitive data from foreign adversaries) before the date of the enactment of this Act shall continue in effect on and after the date of the enactment of this Act. In carrying out the requirements of this Act, the Secretary may amend regulations or promulgate new regulations and procedures as the Secretary considers appropriate.

(b) GUIDANCE.—The Secretary may issue guidance and establish procedures to carry out this Act.

(c) TECHNICAL ADVISORY COMMITTEE.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall establish an ICTS technical advisory committee to report to the Executive Director of the Office of Information and Communications Technology and Services.

(d) MEMBERSHIP.—The ICTS advisory committee shall include the following:

(1) Industry academic experts on covered ICTS transaction supply chains.

(2) Representatives of private sector companies, industry associations, and academia.

(3) A designated Federal officer to administer the advisory committee and report to the Executive Director.

(e) CONFIDENTIALITY AND DISCLOSURE OF INFORMATION.—Any information or document not otherwise publicly or commercially available that has been submitted to the Secretary under this Act shall not be released publicly excepted to the extent required by Federal law.

SEC. 7. ENFORCEMENT.

(a) INVESTIGATIONS.—

(1) IN GENERAL.—The Secretary may conduct an investigation of any violation of an authorization, order, mitigation measure, regulation, or prohibition issued under this Act.

(2) ACTIONS BY DESIGNEES.—In conducting an investigation described in paragraph (1), designated officers or employees of the Secretary may, to the extent necessary or appropriate to enforce this Act, exercise such authority as is conferred upon them by any other Federal law, subject to policies and procedures approved by the Attorney General.

(b) PERMITTED ACTIVITIES.—An officer or employee authorized to conduct investigations under subsection (a) by the Secretary may do any of the following:

(1) Inspect, search, detain, seize, or impose a temporary denial order with respect to any item, in any form, or conveyance on which it is believed that there are items that have been, are being, or are about to be imported into the United States in violation of this Act or any other applicable Federal law.

(2) Require, inspect, and obtain any book, record, and any other information from any person subject to the provisions of this Act or other applicable Federal law.

(3) Administer an oath or affirmation and, by subpoena, require any person to appear and testify or to appear and produce books, records, and other writings.

(4) Obtain a court order and issue legal process to the extent authorized under chapters 119, 121, and 206 of title 18, United States Code, or any other applicable Federal law.

(c) ENFORCEMENT OF SUBPOENAS.—In the case of contumacy by, or refusal to obey a subpoena issued to, any person under subsection (b)(3), a district court of the United States, after notice to such person and a hearing,

shall have jurisdiction to issue an order requiring such person to appear and give testimony or to appear and produce books, records, and other writings, regardless of format, that are the subject of the subpoena. Any failure to obey such order of the court may be punished by such court as a contempt thereof.

(d) ACTIONS BY THE ATTORNEY GENERAL.—The Attorney General may bring an action in an appropriate district court of the United States for appropriate relief, including declaratory and injunctive, or divestment relief, against any person who violates this Act or any regulation, order, direction, mitigation measure, prohibition, or other authorization or directive issued under this Act.

SEC. 8. JUDICIAL REVIEW.

(a) RIGHT OF ACTION.—A claim or petition challenging this Act or any action, finding, or determination under this Act may be filed only in the United States Court of Appeals for the District of Columbia Circuit.

(b) EXCLUSIVE JURISDICTION.—The United States Court of Appeals for the District of Columbia Circuit shall have exclusive jurisdiction over claims or petitions arising under this Act against the United States, any agency, or any component or official of an agency, subject to review by the Supreme Court of the United States under section 1254 of title 28, United States Code.

(c) IN CAMERA AND EX PARTE REVIEW.—The following information may be included in the administrative record and shall be submitted only to the court ex parte and in camera:

(1) Sensitive security information, as defined in section 1520.5 of title 49, Code of Federal Regulations.

(2) Records or information compiled for law enforcement purposes, as described in section 552(b)(7) of title 5, United States Code.

(3) Classified information, meaning any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014).

(4) Information subject to privilege or protections under any other provision of law, including subchapter II of title 31, United States Code.

(d) INFORMATION UNDER SEAL.—Any information that is part of the administrative record filed ex parte and in camera under subsection (b), or cited by the court in any decision, shall be treated by the court consistent with

the provisions of this section. In no event shall such information be released to the claimant or petitioner or as part of the public record.

(e) RETURN.—After the expiration of the time to seek further review, or the conclusion of further proceedings, the court shall return the administrative record, including any and all copies, to the United States.

(f) EXCLUSIVE REMEDY.—A determination by the court under this section shall be the exclusive judicial remedy for any claim or petition for review challenging this Act or any action, finding, or determination under this Act against the United States, any agency, or any component or official of any such agency.

(g) RULE OF CONSTRUCTION.—Nothing in this section shall be construed as limiting, superseding, or preventing the invocation of, any privileges or defenses that are otherwise available at law or in equity to protect against the disclosure of information.

(h) STATUTE OF LIMITATIONS.—A challenge to any determination under this Act may only be brought not later than 180 days after the date of such a determination.

SEC. 9. PENALTIES.

(a) UNLAWFUL ACTS.—It shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any regulation, order, direction, prohi-

bition, or other authorization or directive issued under this Act.

(b) CRIMINAL PENALTIES.—A person who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids and abets in the commission of a violation of subsection (a) shall be fined not more than $1,000,000 for each violation, imprisoned for not more than 20 years, or both.

(c) CIVIL PENALTIES.—The Secretary may impose the following civil penalties on a person for each violation by that person of a rule promulgated under this section:

(1) A fine that is the greater of—

(A) $300,000; or

(B) an amount that is twice the value of the action that is the basis of the violation with respect to which the penalty is imposed.

(2) Revocation of any mitigation measure or authorization issued under this Act to the person.

(3) A prohibition or other restriction on the ability of the person to engage in any transaction or class of transactions covered by this Act.

(d) PROCEDURES.—Any civil penalty imposed under subsection (c) may be imposed only pursuant to a rule promulgated under this section.

(e) STANDARDS FOR LEVELS OF CIVIL PENALTY.—The Secretary may, by rule, provide standards for establishing levels of civil penalty under subsection (c) based upon factors, including—

(1) the seriousness of the violation;

(2) the culpability of the violator, including any pattern of reckless behavior; and

(3) any mitigating factors, such as the record of cooperation of the violator with the Federal Government in disclosing the violation.

SEC. 10. RELATIONSHIP TO OTHER LAWS.

(a) RULE OF CONSTRUCTION RELATING TO OTHER LAW.—Nothing in this Act shall be construed to alter or affect any other authority, process, regulation, investigation, enforcement measure, or review provided by or established under any other provision of Federal law.

(b) ADMINISTRATIVE PROCEDURE EXCEPTIONS.—Except with respect to a civil penalty imposed pursuant to section 9(c), any function exercised under this Act is not subject to sections 551, 553 through 559, and 701 through 706 of title 5, United States Code.

(c) PAPERWORK REDUCTION ACT EXCEPTION.—The requirements of chapter 35 of title 44, United States Code (commonly referred to as the ''Paperwork Reduction

Act''), shall not apply to any action by the Secretary to implement this Act.

(d) DEFENSE PRODUCTION ACT.—Nothing in this Act shall prevent or preclude the President or the Committee on Foreign Investment in the United States from exercising any authority under section 721 of the Defense Production Act of 1950 (50 U.S.C. 4565 et seq.) as would be available in the absence of this Act.

(e) RULE OF CONSTRUCTION FOR THE OICTS.—Nothing in this Act may be construed as altering any of the authority of the Office of Information and Communications Technology and Services under Executive Order 13873 (84 Fed. Reg. 22689; relating to securing the information and communications technology and services supply chain) and Executive Order 14034 (86 Fed. Reg. 31423; relating to protecting Americans' sensitive data from foreign adversaries).

SEC. 11. DEFINITIONS.

In this Act:

(1) AGENCY.—The term ''agency'' has the meaning given that term in section 551 of title 5, United States Code.

(2) COVERED ICTS TRANSACTION.—The term ''covered ICTS transaction'' means an ICTS transaction that meets each of the following requirements:

(A) Is conducted by any person subject to the jurisdiction of the United States or involves property subject to the jurisdiction of the United States.

(B) Involves ICTS designed, developed, manufactured, or supplied by a person owned by, controlled by, or subject to the jurisdiction or direction of a person or jurisdiction of concern.

(C) Is used in a covered motor vehicle.

(3) COVERED MOTOR VEHICLE.—

(A) IN GENERAL.—The term ''covered motor vehicle'' means a motor vehicle that has one or more integrated systems capable of communicating wirelessly with any other network or device.

(B) MOTOR VEHICLE.—The term ''motor vehicle''—

(i) means a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways; and

(ii) does not include a vehicle operated only on a rail line.

(4) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters.

(5) ICTS TRANSACTION.—The term ''ICTS transaction'' means any acquisition, importation, transfer, installation, dealing in, or use of ICTS, including any ongoing activity, such as a managed service, data transmission, software update, repair, or the platforming or data hosting of an application for consumer download, and any class of ICTS transactions (including the acquisition, importation, transfer, installation, dealing in, or use, including any ongoing activity, of any category of technology product or services, or group of technology products or services as identified by the Secretary).

(6) INFORMATION AND COMMUNICATIONS TECHNOLOGY AND SERVICES; ICTS.—The terms ''information and communications technology or services'' and ''ICTS'' mean any hardware, software, or other product or service, including cloud-computing

services, primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means (including electromagnetic, magnetic, and photonic), including transmission, storage, or display.

(7) OFFICE.—The term ''Office'' means the Office of Information and Communications Technology and Services established under section 2.

(8) PERSON OR JURISDICTION OF CONCERN.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''person or jurisdiction of concern'' means any foreign person or any foreign region, country, or government that is engaged in any long-term pattern or serious instances of activity adverse to the national security of the United States, the security of critical infrastructure of the United States, or the safety and security of United States persons and includes the following:

(i) The Russian Federation.

(ii) The People's Republic of China, including the Hong Kong Special Administrative Region and the Macau Special Administrative Region.

(iii) The Republic of Cuba.

(iv) The Islamic Republic of Iran.

(v) The Democratic People's Republic of Korea.

(vi) Venezuelan politician Nicolás Maduro.

(B) UPDATES TO THE LIST.—The Secretary, in consultation with the Director of National Intelligence, shall periodically review the list under subparagraph (A) and may update by adding to, subtracting from, supplementing, or otherwise amending the list through publication of a notice in the Federal Register and any such update shall apply with respect to any ICTS transaction that is initiated, pending, or completed on or after the date of the notice.

(9) RELEVANT COMMITTEES OF CONGRESS.—The term ''relevant committees of Congress'' means—

(A) the Committee on Commerce, Science, and Transportation, the Committee on Banking, Housing, and Urban Affairs, the Committee on Armed Services, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Energy and Commerce, the Committee on Foreign Affairs, the

Committee on Armed Services, and the Permanent Select Committee on Intelligence of the House of Representatives.

(10) SECRETARY.—The term ''Secretary'' means the Secretary of Commerce.

(11) UNDUE OR UNACCEPTABLE RISK.—The term ''undue or unacceptable risk'' means any of the following:

(A) The undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of ICTS in the United States.

(B) The undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States.

(C) The unacceptable risk to the national security of the United States or the security and safety of United States persons.

(12) UNITED STATES PERSON.—The term ''United States person'' any United States citizen, national, or lawful permanent resident, and any corporation, partnership, or other organization organized under the laws of the United States.

○