

118TH CONGRESS
2D SESSION

H. R. 8742

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.

1 *Be it enacted by the Senate and House of Representa-
2 tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Information and Communication Technology and Serv-
6 ices National Security Review Act” or the “ICTS National
7 Security Review Act”.

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

See. 1. Short title; table of contents.
See. 2. The Office of Information and Communications Technology and Services.
See. 3. Transaction review process.
See. 4. Regulating person or jurisdiction of concern-connected covered ICTS transactions.
See. 5. Risk assessment.
See. 6. Other authorities.
See. 7. Enforcement.
See. 8. Judicial review.
See. 9. Penalties.
See. 10. Relationship to other laws.
See. 11. Definitions.

3 **SEC. 2. THE OFFICE OF INFORMATION AND COMMUNICA-
4 TIONS TECHNOLOGY AND SERVICES.**

5 (a) ESTABLISHMENT.—There is established within
6 the Bureau of Industry and Security of the Department
7 of Commerce an Office of Information and Communica-
8 tions Technology and Services (in this section, referred to
9 as the “Office”).

10 (b) EXECUTIVE DIRECTOR.—The head of the Office
11 shall be an Executive Director who reports to the Under
12 Secretary for Industry and Security and shall be des-
13 ignated by the Secretary.

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

19 (d) DUTIES.—The Office shall—

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

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

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

11 **SEC. 3. TRANSACTION REVIEW PROCESS.**

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

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

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

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

1 complete information relative to any such trans-
2 action.

3 (B) Require that any such report take a
4 particular form as directed in a request, regula-
5 tion, or other guidance provided by the Sec-
6 retary, which may be required before, during, or
7 after any such transaction.

8 (C) Through any agency, conduct inves-
9 tigations, hold hearings, administer oaths, ex-
10 amine witnesses, receive evidence, take deposi-
11 tions, and require by subpoena the attendance
12 and testimony of witnesses and the production
13 of any book, contract, letter, paper, and other
14 hard copy or document relating to any matter
15 under investigation, regardless of whether any
16 such report has been required or filed.

17 (b) MITIGATION OF RISK.—

18 (1) IN GENERAL.—If the Secretary finds that a
19 covered ICTS transaction poses an undue or unac-
20 ceptable risk under subsection (a), the Secretary
21 shall mitigate the undue or unacceptable risk de-
22 scribed in paragraph (2) or prohibit such trans-
23 action.

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

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

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

9 (B) Require adherence to certain cyberse-
10 curity standards and other mitigation require-
11 ments determined to be necessary by the Sec-
12 retary.

13 (C) Require the exclusion (in whole or in
14 part) of certain components, including physical
15 parts or hardware, software, digital services,
16 and digital components, of any ICTS or any
17 sub-component of ICTS from any such trans-
18 action.

19 (D) Anything else the Secretary deter-
20 mines to be appropriate or necessary to miti-
21 gate the undue or unacceptable risks.

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

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

3 (A) may prohibit the covered ICTS trans-
4 action;

5 (B) shall notify any party subject to the
6 covered ICTS transaction review of the prohibi-
7 tion; and

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

10 **SEC. 4. REGULATING PERSON OR JURISDICTION OF CON-**
11 **CERN-CONNECTED COVERED ICTS TRANS-**
12 **ACTIONS.**

13 (a) AUTHORIZATION TO ISSUE RULES FOR CERTAIN
14 CLASSES OF COVERED ICTS TRANSACTIONS.—The Sec-
15 retary may determine that, for certain classes of covered
16 ICTS transactions, an ICTS transaction review described
17 under section 3 may not effectively address undue or unac-
18 ceptable risks and may promulgate regulations that do the
19 following:

20 (1) Identify particular covered ICTS trans-
21 actions and person or jurisdiction of concern which
22 warrant particular scrutiny for undue or unaccept-
23 able risk.

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

1 related to entities of concern or for classes of cov-
2 ered ICTS transactions.

3 (3) Establish criteria by which particular cov-
4 ered ICTS transactions or particular classes of par-
5 ticipants in the covered ICTS transaction supply
6 chain may be recognized as categorically included in
7 or as categorically excluded from mitigation meas-
8 ures or prohibitions.

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

12 (5) Establish procedures to authorize or license
13 transactions otherwise prohibited pursuant to a reg-
14 ulation promulgated under this section.

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

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

23 **SEC. 5. RISK ASSESSMENT.**

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

1 ally thereafter, the Director of National Intelligence shall
2 submit to the Secretary a risk assessment that relates to
3 threats posed by persons or jurisdictions of concern to the
4 United States by the supply chain of covered ICTS trans-
5 actions that—

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

9 (2) identifies any person or jurisdiction of con-
10 cern, participants in such supply chain, and covered
11 ICTS transactions or classes of covered ICTS trans-
12 actions posing the highest risks to the national secu-
13 rity of the United States.

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

19 (c) CLASSIFIED ANNEX.—The risk assessment sub-
20 mitted under subsection (b)—

21 (1) may include a classified annex; and
22 (2) shall only include specific participants in
23 such supply chain that pose risk to the national se-
24 curity of the United States in the classified annex.

1 **SEC. 6. OTHER AUTHORITIES.**

2 (a) REGULATIONS.—Any regulation the Secretary
3 promulgated under Executive Order 13873 (84 Fed. Reg.
4 22689; relating to securing the information and commu-
5 nications technology and services supply chain) and Exec-
6 utive Order 14034 (86 Fed. Reg. 31423; relating to pro-
7 tecting Americans' sensitive data from foreign adver-
8 saries) before the date of the enactment of this Act shall
9 continue in effect on and after the date of the enactment
10 of this Act. In carrying out the requirements of this Act,
11 the Secretary may amend regulations or promulgate new
12 regulations and procedures as the Secretary considers ap-
13 propriate.

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

16 (c) TECHNICAL ADVISORY COMMITTEE.—Not later
17 than 180 days after the date of the enactment of this Act,
18 the Secretary shall establish an ICTS technical advisory
19 committee to report to the Executive Director of the Office
20 of Information and Communications Technology and Serv-
21 ices.

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

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

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

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

6 (e) CONFIDENTIALITY AND DISCLOSURE OF INFOR-
7 MATION.—Any information or document not otherwise
8 publicly or commercially available that has been submitted
9 to the Secretary under this Act shall not be released pub-
10 licly excepted to the extent required by Federal law.

11 **SEC. 7. ENFORCEMENT.**

12 (a) INVESTIGATIONS.—

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

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

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

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

10 (2) Require, inspect, and obtain any book,
11 record, and any other information from any person
12 subject to the provisions of this Act or other applica-
13 ble Federal law.

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

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

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

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

7 (d) ACTIONS BY THE ATTORNEY GENERAL.—The At-
8 torney General may bring an action in an appropriate dis-
9 trict court of the United States for appropriate relief, in-
10 cluding declaratory and injunctive, or divestment relief,
11 against any person who violates this Act or any regulation,
12 order, direction, mitigation measure, prohibition, or other
13 authorization or directive issued under this Act.

14 **SEC. 8. JUDICIAL REVIEW.**

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

19 (b) EXCLUSIVE JURISDICTION.—The United States
20 Court of Appeals for the District of Columbia Circuit shall
21 have exclusive jurisdiction over claims or petitions arising
22 under this Act against the United States, any agency, or
23 any component or official of an agency, subject to review
24 by the Supreme Court of the United States under section
25 1254 of title 28, United States Code.

1 (c) IN CAMERA AND EX PARTE REVIEW.—The fol-
2 lowing information may be included in the administrative
3 record and shall be submitted only to the court ex parte
4 and in camera:

5 (1) Sensitive security information, as defined in
6 section 1520.5 of title 49, Code of Federal Regula-
7 tions.

8 (2) Records or information compiled for law en-
9 forcement purposes, as described in section
10 552(b)(7) of title 5, United States Code.

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

19 (4) Information subject to privilege or protec-
20 tions under any other provision of law, including
21 subchapter II of title 31, United States Code.

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

1 the provisions of this section. In no event shall such infor-
2 mation be released to the claimant or petitioner or as part
3 of the public record.

4 (e) RETURN.—After the expiration of the time to
5 seek further review, or the conclusion of further pro-
6 ceedings, the court shall return the administrative record,
7 including any and all copies, to the United States.

8 (f) EXCLUSIVE REMEDY.—A determination by the
9 court under this section shall be the exclusive judicial rem-
10 edy for any claim or petition for review challenging this
11 Act or any action, finding, or determination under this
12 Act against the United States, any agency, or any compo-
13 nent or official of any such agency.

14 (g) RULE OF CONSTRUCTION.—Nothing in this sec-
15 tion shall be construed as limiting, superseding, or pre-
16 venting the invocation of, any privileges or defenses that
17 are otherwise available at law or in equity to protect
18 against the disclosure of information.

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

22 **SEC. 9. PENALTIES.**

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

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

3 (b) CRIMINAL PENALTIES.—A person who willfully
4 commits, willfully attempts to commit, or willfully con-
5 spires to commit, or aids and abets in the commission of
6 a violation of subsection (a) shall be fined not more than
7 \$1,000,000 for each violation, imprisoned for not more
8 than 20 years, or both.

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

12 (1) A fine that is the greater of—

13 (A) \$300,000; or

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

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

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

22 (d) PROCEDURES.—Any civil penalty imposed under
23 subsection (c) may be imposed only pursuant to a rule pro-
24 mulgated under this section.

1 (e) STANDARDS FOR LEVELS OF CIVIL PENALTY.—

2 The Secretary may, by rule, provide standards for estab-
3 lishing levels of civil penalty under subsection (c) based
4 upon factors, including—

5 (1) the seriousness of the violation;

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

8 (3) any mitigating factors, such as the record
9 of cooperation of the violator with the Federal Gov-
10 ernment in disclosing the violation.

11 **SEC. 10. RELATIONSHIP TO OTHER LAWS.**

12 (a) RULE OF CONSTRUCTION RELATING TO OTHER
13 LAW.—Nothing in this Act shall be construed to alter or
14 affect any other authority, process, regulation, investiga-
15 tion, enforcement measure, or review provided by or estab-
16 lished under any other provision of Federal law.

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

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

1 Act”), shall not apply to any action by the Secretary to
2 implement this Act.

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

9 (e) RULE OF CONSTRUCTION FOR THE OICTS.—
10 Nothing in this Act may be construed as altering any of
11 the authority of the Office of Information and Commu-
12 nications Technology and Services under Executive Order
13 13873 (84 Fed. Reg. 22689; relating to securing the infor-
14 mation and communications technology and services sup-
15 ply chain) and Executive Order 14034 (86 Fed. Reg.
16 31423; relating to protecting Americans’ sensitive data
17 from foreign adversaries).

18 **SEC. 11. DEFINITIONS.**

19 In this Act:

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

23 (2) COVERED ICTS TRANSACTION.—The term
24 “covered ICTS transaction” means an ICTS trans-
25 action that—

1 transfer, installation, dealing in, or use, including
2 any ongoing activity, of any category of technology
3 product or services, or group of technology products
4 or services as identified by the Secretary).

5 (5) INFORMATION AND COMMUNICATIONS
6 TECHNOLOGY AND SERVICES; ICTS.—The terms “in-
7 formation and communications technology or serv-
8 ices” and “ICTS” mean any hardware, software, or
9 other product or service, including cloud-computing
10 services, primarily intended to fulfill or enable the
11 function of information or data processing, storage,
12 retrieval, or communication by electronic means (in-
13 cluding electromagnetic, magnetic, and photonic), in-
14 cluding transmission, storage, or display.

15 (6) OFFICE.—The term “Office” means the Of-
16 fice of Information and Communications Technology
17 and Services established under section 2.

18 (7) PERSON OR JURISDICTION OF CONCERN.—
19 (A) IN GENERAL.—Except as provided in
20 subparagraph (B), the term “person or jurisdic-
21 tion of concern” means any foreign person or
22 any foreign region, country, or government that
23 is engaged in any long-term pattern or serious
24 instances of activity adverse to the national se-
25 curity of the United States, the security of crit-

1 ical infrastructure of the United States, or the
2 safety and security of United States persons
3 and includes the following:

4 (i) The Russian Federation.
5 (ii) The People's Republic of China,
6 including the Hong Kong Special Adminis-
7 trative Region and the Macau Special Ad-
8 ministrative Region.

9 (iii) The Republic of Cuba.
10 (iv) The Islamic Republic of Iran.
11 (v) The Democratic People's Republic
12 of Korea.

13 (vi) Venezuelan politician Nicolás
14 Maduro.

15 (B) UPDATES TO THE LIST.—The Sec-
16 retary, in consultation with the Director of Na-
17 tional Intelligence, shall periodically review the
18 list under subparagraph (A) and may update by
19 adding to, subtracting from, supplementing, or
20 otherwise amending the list through publication
21 of a notice in the Federal Register and any
22 such update shall apply with respect to any
23 ICTS transaction that is initiated, pending, or
24 completed on or after the date of the notice.

1 (8) RELEVANT COMMITTEES OF CONGRESS.—

2 The term “relevant committees of Congress”
3 means—4 (A) the Committee on Commerce, Science,
5 and Transportation, the Committee on Bank-
6 ing, Housing, and Urban Affairs, the Com-
7 mittee on Armed Services, and the Select Com-
8 mittee on Intelligence of the Senate; and9 (B) the Committee on Energy and Com-
10 merce, the Committee on Foreign Affairs, the
11 Committee on Armed Services, and the Perma-
12 nent Select Committee on Intelligence of the
13 House of Representatives.14 (9) SECRETARY.—The term “Secretary” means
15 the Secretary of Commerce.16 (10) UNDUE OR UNACCEPTABLE RISK.—The
17 term “undue or unacceptable risk” means any of the
18 following:19 (A) The undue risk of sabotage to or sub-
20 version of the design, integrity, manufacturing,
21 production, distribution, installation, operation,
22 or maintenance of ICTS in the United States.23 (B) The undue risk of catastrophic effects
24 on the security or resiliency of United States

1 critical infrastructure or the digital economy of
2 the United States.

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

6 (11) UNITED STATES PERSON.—The term
7 “United States person” any United States citizen,
8 national, or lawful permanent resident, and any cor-
9 poration, partnership, or other organization orga-
10 nized under the laws of the United States.

