

115TH CONGRESS
2D SESSION

H. R. _____

To require the Secretary of Homeland Security to establish a security vulnerability disclosure policy, to establish a bug bounty program for the Department of Homeland Security, to amend title 41, United States Code, to provide for Federal acquisition supply chain security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

M. _____ introduced the following bill; which was referred to the
Committee on _____

A BILL

To require the Secretary of Homeland Security to establish a security vulnerability disclosure policy, to establish a bug bounty program for the Department of Homeland Security, to amend title 41, United States Code, to provide for Federal acquisition supply chain security, 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 “Strengthening and Enhancing Cyber-capabilities by Uti-

1 lizing Risk Exposure Technology Act” or the “SECURE
2 Technology Act”.

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

Sec. 1. Short title; table of contents.

TITLE I—DEPARTMENT OF HOMELAND SECURITY INFORMATION
SECURITY AND OTHER MATTERS

Sec. 101. Department of Homeland Security disclosure of security
vulnerabilities.

Sec. 102. Department of Homeland Security bug bounty pilot program.

Sec. 103. Congressional submittal of reports relating to certain special access
programs and similar programs.

TITLE II—FEDERAL ACQUISITION SUPPLY CHAIN SECURITY

Sec. 201. Short title.

Sec. 202. Federal acquisition supply chain security.

Sec. 203. Authorities of executive agencies relating to mitigating supply chain
risks in the procurement of covered articles.

Sec. 204. Federal Information Security Modernization Act.

Sec. 205. Effective date.

5 **TITLE I—DEPARTMENT OF**
6 **HOMELAND SECURITY INFOR-**
7 **MATION SECURITY AND**
8 **OTHER MATTERS**

9 **SEC. 101. DEPARTMENT OF HOMELAND SECURITY DISCLO-**
10 **SURE OF SECURITY VULNERABILITIES.**

11 (a) VULNERABILITY DISCLOSURE POLICY.—The Sec-
12 retary of Homeland Security shall establish a policy appli-
13 cable to individuals, organizations, and companies that re-
14 port security vulnerabilities on appropriate information
15 systems of Department of Homeland Security. Such policy
16 shall include each of the following:

1 (1) The appropriate information systems of the
2 Department that individuals, organizations, and
3 companies may use to discover and report security
4 vulnerabilities on appropriate information systems.

5 (2) The conditions and criteria under which in-
6 dividuals, organizations, and companies may operate
7 to discover and report security vulnerabilities.

8 (3) How individuals, organizations, and compa-
9 nies may disclose to the Department security
10 vulnerabilities discovered on appropriate information
11 systems of the Department.

12 (4) The ways in which the Department may
13 communicate with individuals, organizations, and
14 companies that report security vulnerabilities.

15 (5) The process the Department shall use for
16 public disclosure of reported security vulnerabilities.

17 (b) REMEDIATION PROCESS.—The Secretary of
18 Homeland Security shall develop a process for the Depart-
19 ment of Homeland Security to address the mitigation or
20 remediation of the security vulnerabilities reported
21 through the policy developed in subsection (a).

22 (c) CONSULTATION.—

23 (1) IN GENERAL.—In developing the security
24 vulnerability disclosure policy under subsection (a),

1 the Secretary of Homeland Security shall consult
2 with each of the following:

3 (A) The Attorney General regarding how
4 to ensure that individuals, organizations, and
5 companies that comply with the requirements of
6 the policy developed under subsection (a) are
7 protected from prosecution under section 1030
8 of title 18, United States Code, civil lawsuits,
9 and similar provisions of law with respect to
10 specific activities authorized under the policy.

11 (B) The Secretary of Defense and the Ad-
12 ministrator of General Services regarding les-
13 sons that may be applied from existing vulner-
14 ability disclosure policies.

15 (C) Non-governmental security researchers.

16 (2) NONAPPLICABILITY OF FACA.—The Federal
17 Advisory Committee Act (5 U.S.C. App.) shall not
18 apply to any consultation under this section.

19 (d) PUBLIC AVAILABILITY.—The Secretary of Home-
20 land Security shall make the policy developed under sub-
21 section (a) publicly available.

22 (e) SUBMISSION TO CONGRESS.—

23 (1) DISCLOSURE POLICY AND REMEDIATION
24 PROCESS.—Not later than 90 days after the date of
25 the enactment of this Act, the Secretary of Home-

1 land Security shall submit to the appropriate con-
2 gressional committees a copy of the policy required
3 under subsection (a) and the remediation process re-
4 quired under subsection (b).

5 (2) REPORT AND BRIEFING.—

6 (A) REPORT.—Not later than one year
7 after establishing the policy required under sub-
8 section (a), the Secretary of Homeland Security
9 shall submit to the appropriate congressional
10 committees a report on such policy and the re-
11 mediation process required under subsection
12 (b).

13 (B) ANNUAL BRIEFINGS.—One year after
14 the date of the submission of the report under
15 subparagraph (A), and annually thereafter for
16 each of the next three years, the Secretary of
17 Homeland Security shall provide to the appro-
18 priate congressional committees a briefing on
19 the policy required under subsection (a) and the
20 process required under subsection (b).

21 (C) MATTERS FOR INCLUSION.—The re-
22 port required under subparagraph (A) and the
23 briefings required under subparagraph (B) shall
24 include each of the following with respect to the
25 policy required under subsection (a) and the

1 process required under subsection (b) for the
2 period covered by the report or briefing, as the
3 case may be:

4 (i) The number of unique security
5 vulnerabilities reported.

6 (ii) The number of previously un-
7 known security vulnerabilities mitigated or
8 remediated.

9 (iii) The number of unique individ-
10 uals, organizations, and companies that re-
11 ported security vulnerabilities.

12 (iv) The average length of time be-
13 tween the reporting of security
14 vulnerabilities and mitigation or remedi-
15 ation of such vulnerabilities.

16 (f) DEFINITIONS.—In this section:

17 (1) The term “security vulnerability” has the
18 meaning given that term in section 102(17) of the
19 Cybersecurity Information Sharing Act of 2015 (6
20 U.S.C. 1501(17)), in information technology.

21 (2) The term “information system” has the
22 meaning given that term by section 3502 of title 44,
23 United States Code.

24 (3) The term “appropriate information system”
25 means an information system that the Secretary of

1 Homeland Security selects for inclusion under the
2 vulnerability disclosure policy required by subsection
3 (a).

4 (4) The term “appropriate congressional com-
5 mittees” means—

6 (A) the Committee on Homeland Security,
7 the Committee on Armed Services, the Com-
8 mittee on Energy and Commerce, and the Per-
9 manent Select Committee on Intelligence of the
10 House of Representatives; and

11 (B) the Committee on Homeland Security
12 and Governmental Affairs, the Committee on
13 Armed Services, the Committee on Commerce,
14 Science, and Transportation, and the Select
15 Committee on Intelligence of the Senate.

16 **SEC. 102. DEPARTMENT OF HOMELAND SECURITY BUG**
17 **BOUNTY PILOT PROGRAM.**

18 (a) **DEFINITIONS.**—In this section:

19 (1) The term “appropriate congressional com-
20 mittees” means—

21 (A) the Committee on Homeland Security
22 and Governmental Affairs of the Senate;

23 (B) the Select Committee on Intelligence
24 of the Senate;

1 (C) the Committee on Homeland Security
2 of the House of Representatives; and

3 (D) Permanent Select Committee on Intel-
4 ligence of the House of Representatives.

5 (2) The term “bug bounty program” means a
6 program under which—

7 (A) individuals, organizations, and compa-
8 nies are temporarily authorized to identify and
9 report vulnerabilities of appropriate information
10 systems of the Department; and

11 (B) eligible individuals, organizations, and
12 companies receive compensation in exchange for
13 such reports.

14 (3) The term “Department” means the Depart-
15 ment of Homeland Security.

16 (4) The term “eligible individual, organization,
17 or company” means an individual, organization, or
18 company that meets such criteria as the Secretary
19 determines in order to receive compensation in com-
20 pliance with Federal laws.

21 (5) The term “information system” has the
22 meaning given the term in section 3502 of title 44,
23 United States Code.

1 (6) The term “pilot program” means the bug
2 bounty pilot program required to be established
3 under subsection (b)(1).

4 (7) The term “Secretary” means the Secretary
5 of Homeland Security.

6 (b) BUG BOUNTY PILOT PROGRAM.—

7 (1) ESTABLISHMENT.—Not later than 180 days
8 after the date of enactment of this Act, the Sec-
9 retary shall establish, within the Office of the Chief
10 Information Officer, a bug bounty pilot program to
11 minimize vulnerabilities of appropriate information
12 systems of the Department.

13 (2) RESPONSIBILITIES OF SECRETARY.—In es-
14 tablishing and conducting the pilot program, the
15 Secretary shall—

16 (A) designate appropriate information sys-
17 tems to be included in the pilot program;

18 (B) provide compensation to eligible indi-
19 viduals, organizations, and companies for re-
20 ports of previously unidentified security
21 vulnerabilities within the information systems
22 designated under subparagraph (A);

23 (C) establish criteria for individuals, orga-
24 nizations, and companies to be considered eligi-

1 ble for compensation under the pilot program in
2 compliance with Federal laws;

3 (D) consult with the Attorney General on
4 how to ensure that approved individuals, orga-
5 nizations, or companies that comply with the
6 requirements of the pilot program are protected
7 from prosecution under section 1030 of title 18,
8 United States Code, and similar provisions of
9 law, and civil lawsuits for specific activities au-
10 thorized under the pilot program;

11 (E) consult with the Secretary of Defense
12 and the heads of other departments and agen-
13 cies that have implemented programs to provide
14 compensation for reports of previously undis-
15 closed vulnerabilities in information systems, re-
16 garding lessons that may be applied from such
17 programs; and

18 (F) develop an expeditious process by
19 which an individual, organization, or company
20 can register with the Department, submit to a
21 background check as determined by the Depart-
22 ment, and receive a determination as to eligi-
23 bility; and

24 (G) engage qualified interested persons, in-
25 cluding non-government sector representatives,

1 about the structure of the pilot program as con-
2 structive and to the extent practicable.

3 (3) CONTRACT AUTHORITY.—In establishing
4 the pilot program, the Secretary, subject to the
5 availability of appropriations, may award 1 or more
6 competitive contracts to an entity, as necessary, to
7 manage the pilot program.

8 (c) REPORT TO CONGRESS.—Not later than 180 days
9 after the date on which the pilot program is completed,
10 the Secretary shall submit to the appropriate congres-
11 sional committees a report on the pilot program, which
12 shall include—

13 (1) the number of individuals, organizations, or
14 companies that participated in the pilot program,
15 broken down by the number of individuals, organiza-
16 tions, or companies that—

17 (A) registered;

18 (B) were determined eligible;

19 (C) submitted security vulnerabilities; and

20 (D) received compensation;

21 (2) the number and severity of vulnerabilities
22 reported as part of the pilot program;

23 (3) the number of previously unidentified secu-
24 rity vulnerabilities remediated as a result of the pilot
25 program;

1 (A) by redesignating paragraphs (1) and
2 (2) as paragraphs (2) and (3), respectively; and

3 (B) by inserting before paragraph (2), as
4 so redesignated, the following:

5 “(1) CONGRESSIONAL OVERSIGHT COMMIT-
6 TEES.—The term ‘congressional oversight commit-
7 tees’ means—

8 “(A) congressional leadership and author-
9 izing and appropriations congressional commit-
10 tees with jurisdiction or shared jurisdiction over
11 a department or agency;

12 “(B) the Committee on Homeland Security
13 and Governmental Affairs of the Senate; and

14 “(C) the Committee on Oversight and Gov-
15 ernment Reform of the House of Representa-
16 tives.”.

17 **TITLE II—FEDERAL ACQUISI-**
18 **TION SUPPLY CHAIN SECU-**
19 **RITY**

20 **SEC. 201. SHORT TITLE.**

21 This title may be cited as the “Federal Acquisition
22 Supply Chain Security Act of 2018”.

1 **SEC. 202. FEDERAL ACQUISITION SUPPLY CHAIN SECURITY.**

2 (a) IN GENERAL.—Chapter 13 of title 41, United
3 States Code, is amended by adding at the end the fol-
4 lowing new subchapter:

5 “SUBCHAPTER III—FEDERAL ACQUISITION
6 SUPPLY CHAIN SECURITY

7 “§ 1321. Definitions

8 “In this subchapter:

9 “(1) APPROPRIATE CONGRESSIONAL COMMIT-
10 TEES AND LEADERSHIP.—The term ‘appropriate
11 congressional committees and leadership’ means—

12 “(A) the Committee on Homeland Security
13 and Governmental Affairs, the Committee on
14 the Judiciary, the Committee on Appropria-
15 tions, the Committee on Armed Services, the
16 Committee on Commerce, Science, and Trans-
17 portation, the Select Committee on Intelligence,
18 and the majority and minority leader of the
19 Senate; and

20 “(B) the Committee on Oversight and Gov-
21 ernment Reform, the Committee on the Judici-
22 ary, the Committee on Appropriations, the
23 Committee on Homeland Security, the Com-
24 mittee on Armed Services, the Committee on
25 Energy and Commerce, the Permanent Select
26 Committee on Intelligence, and the Speaker and

1 minority leader of the House of Representa-
2 tives.

3 “(2) COUNCIL.—The term ‘Council’ means the
4 Federal Acquisition Security Council established
5 under section 1322(a) of this title.

6 “(3) COVERED ARTICLE.—The term ‘covered
7 article’ has the meaning given that term in section
8 4713 of this title.

9 “(4) COVERED PROCUREMENT ACTION.—The
10 term ‘covered procurement action’ has the meaning
11 given that term in section 4713 of this title.

12 “(5) INFORMATION AND COMMUNICATIONS
13 TECHNOLOGY.—The term ‘information and commu-
14 nications technology’ has the meaning given that
15 term in section 4713 of this title.

16 “(6) INTELLIGENCE COMMUNITY.—The term
17 ‘intelligence community’ has the meaning given that
18 term in section 3(4) of the National Security Act of
19 1947 (50 U.S.C. 3003(4)).

20 “(7) NATIONAL SECURITY SYSTEM.—The term
21 ‘national security system’ has the meaning given
22 that term in section 3552 of title 44.

23 “(8) SUPPLY CHAIN RISK.—The term ‘supply
24 chain risk’ has the meaning given that term in sec-
25 tion 4713 of this title.

1 **“§ 1322. Federal Acquisition Security Council estab-**
2 **lishment and membership**

3 “(a) ESTABLISHMENT.—There is established in the
4 executive branch a Federal Acquisition Security Council.

5 “(b) MEMBERSHIP.—

6 “(1) IN GENERAL.—The following agencies
7 shall be represented on the Council:

8 “(A) The Office of Management and
9 Budget.

10 “(B) The General Services Administration.

11 “(C) The Department of Homeland Secu-
12 rity, including the Cybersecurity and Infra-
13 structure Security Agency.

14 “(D) The Office of the Director of Na-
15 tional Intelligence, including the National Coun-
16 terintelligence and Security Center.

17 “(E) The Department of Justice, including
18 the Federal Bureau of Investigation.

19 “(F) The Department of Defense, includ-
20 ing the National Security Agency.

21 “(G) The Department of Commerce, in-
22 cluding the National Institute of Standards and
23 Technology.

24 “(H) Such other executive agencies as de-
25 termined by the Chairperson of the Council.

26 “(2) LEAD REPRESENTATIVES.—

1 “(A) DESIGNATION.—

2 “(i) IN GENERAL.—Not later than 45
3 days after the date of the enactment of the
4 Federal Acquisition Supply Chain Security
5 Act of 2018, the head of each agency rep-
6 resented on the Council shall designate a
7 representative of that agency as the lead
8 representative of the agency on the Coun-
9 cil.

10 “(ii) REQUIREMENTS.—The rep-
11 resentative of an agency designated under
12 clause (i) shall have expertise in supply
13 chain risk management, acquisitions, or in-
14 formation and communications technology.

15 “(B) FUNCTIONS.—The lead representa-
16 tive of an agency designated under subpara-
17 graph (A) shall ensure that appropriate per-
18 sonnel, including leadership and subject matter
19 experts of the agency, are aware of the business
20 of the Council.

21 “(c) CHAIRPERSON.—

22 “(1) DESIGNATION.—Not later than 45 days
23 after the date of the enactment of the Federal Ac-
24 quisition Supply Chain Security Act of 2018, the Di-
25 rector of the Office of Management and Budget

1 shall designate a senior-level official from the Office
2 of Management and Budget to serve as the Chair-
3 person of the Council.

4 “(2) FUNCTIONS.—The Chairperson shall per-
5 form functions that include—

6 “(A) subject to subsection (d), developing
7 a schedule for meetings of the Council;

8 “(B) designating executive agencies to be
9 represented on the Council under subsection
10 (b)(1)(H);

11 “(C) in consultation with the lead rep-
12 resentative of each agency represented on the
13 Council, developing a charter for the Council;
14 and

15 “(D) not later than 7 days after comple-
16 tion of the charter, submitting the charter to
17 the appropriate congressional committees and
18 leadership.

19 “(d) MEETINGS.—The Council shall meet not later
20 than 60 days after the date of the enactment of the Fed-
21 eral Acquisition Supply Chain Security Act of 2018 and
22 not less frequently than quarterly thereafter.

23 **“§ 1323. Functions and authorities**

24 “(a) IN GENERAL.—The Council shall perform func-
25 tions that include the following:

1 “(1) Identifying and recommending develop-
2 ment by the National Institute of Standards and
3 Technology of supply chain risk management stand-
4 ards, guidelines, and practices for executive agencies
5 to use when assessing and developing mitigation
6 strategies to address supply chain risks, particularly
7 in the acquisition and use of covered articles under
8 section 1326(a) of this title.

9 “(2) Identifying or developing criteria for shar-
10 ing information with executive agencies, other Fed-
11 eral entities, and non-Federal entities with respect to
12 supply chain risk, including information related to
13 the exercise of authorities provided under this sec-
14 tion and sections 1326 and 4713 of this title. At a
15 minimum, such criteria shall address—

16 “(A) the content to be shared;

17 “(B) the circumstances under which shar-
18 ing is mandated or voluntary; and

19 “(C) the circumstances under which it is
20 appropriate for an executive agency to rely on
21 information made available through such shar-
22 ing in exercising the responsibilities and au-
23 thorities provided under this section and section
24 4713 of this title.

1 “(3) Identifying an appropriate executive agen-
2 cy to—

3 “(A) accept information submitted by execu-
4 tive agencies based on the criteria established
5 under paragraph (2);

6 “(B) facilitate the sharing of information
7 received under subparagraph (A) to support
8 supply chain risk analyses under section 1326
9 of this title, recommendations under this sec-
10 tion, and covered procurement actions under
11 section 4713 of this title;

12 “(C) share with the Council information
13 regarding covered procurement actions by execu-
14 tive agencies taken under section 4713 of this
15 title; and

16 “(D) inform the Council of orders issued
17 under this section.

18 “(4) Identifying, as appropriate, executive agen-
19 cies to provide—

20 “(A) shared services, such as support for
21 making risk assessments, validation of products
22 that may be suitable for acquisition, and miti-
23 gation activities; and

24 “(B) common contract solutions to support
25 supply chain risk management activities, such

1 as subscription services or machine-learning-en-
2 hanced analysis applications to support in-
3 formed decision making.

4 “(5) Identifying and issuing guidance on addi-
5 tional steps that may be necessary to address supply
6 chain risks arising in the course of executive agen-
7 cies providing shared services, common contract so-
8 lutions, acquisitions vehicles, or assisted acquisitions.

9 “(6) Engaging with the private sector and other
10 nongovernmental stakeholders in performing the
11 functions described in paragraphs (1) and (2) and
12 on issues relating to the management of supply
13 chain risks posed by the acquisition of covered arti-
14 cles.

15 “(7) Carrying out such other actions, as deter-
16 mined by the Council, that are necessary to reduce
17 the supply chain risks posed by acquisitions and use
18 of covered articles.

19 “(b) PROGRAM OFFICE AND COMMITTEES.—The
20 Council may establish a program office and any commit-
21 tees, working groups, or other constituent bodies the
22 Council deems appropriate, in its sole and unreviewable
23 discretion, to carry out its functions.

24 “(c) AUTHORITY FOR EXCLUSION OR REMOVAL OR-
25 DERS.—

1 “(1) CRITERIA.—To reduce supply chain risk,
2 the Council shall establish criteria and procedures
3 for—

4 “(A) recommending orders applicable to
5 executive agencies requiring the exclusion of
6 sources or covered articles from executive agen-
7 cy procurement actions (in this section referred
8 to as ‘exclusion orders’);

9 “(B) recommending orders applicable to
10 executive agencies requiring the removal of cov-
11 ered articles from executive agency information
12 systems (in this section referred to as ‘removal
13 orders’);

14 “(C) requesting and approving exceptions
15 to an issued exclusion or removal order when
16 warranted by circumstances, including alter-
17 native mitigation actions or other findings relat-
18 ing to the national interest, including national
19 security reviews, national security investiga-
20 tions, or national security agreements; and

21 “(D) ensuring that recommended orders do
22 not conflict with standards and guidelines
23 issued under section 11331 of title 40 and that
24 the Council consults with the Director of the
25 National Institute of Standards and Technology

1 regarding any recommended orders that would
2 implement standards and guidelines developed
3 by the National Institute of Standards and
4 Technology.

5 “(2) RECOMMENDATIONS.—The Council shall
6 use the criteria established under paragraph (1), in-
7 formation made available under subsection (a)(3),
8 and any other information the Council determines
9 appropriate to issue recommendations, for applica-
10 tion to executive agencies or any subset thereof, re-
11 garding the exclusion of sources or covered articles
12 from any executive agency procurement action, in-
13 cluding source selection and consent for a contractor
14 to subcontract, or the removal of covered articles
15 from executive agency information systems. Such
16 recommendations shall include—

17 “(A) information necessary to positively
18 identify the sources or covered articles rec-
19 ommended for exclusion or removal;

20 “(B) information regarding the scope and
21 applicability of the recommended exclusion or
22 removal order;

23 “(C) a summary of any risk assessment re-
24 viewed or conducted in support of the rec-
25 ommended exclusion or removal order;

1 “(D) a summary of the basis for the rec-
2 ommendation, including a discussion of less in-
3 trusive measures that were considered and why
4 such measures were not reasonably available to
5 reduce supply chain risk;

6 “(E) a description of the actions necessary
7 to implement the recommended exclusion or re-
8 moval order; and

9 “(F) where practicable, in the Council’s
10 sole and unreviewable discretion, a description
11 of mitigation steps that could be taken by the
12 source that may result in the Council rescinding
13 a recommendation.

14 “(3) NOTICE OF RECOMMENDATION AND RE-
15 VIEW.—A notice of the Council’s recommendation
16 under paragraph (2) shall be issued to any source
17 named in the recommendation advising—

18 “(A) that a recommendation has been
19 made;

20 “(B) of the criteria the Council relied upon
21 under paragraph (1) and, to the extent con-
22 sistent with national security and law enforce-
23 ment interests, of information that forms the
24 basis for the recommendation;

1 “(C) that, within 30 days after receipt of
2 notice, the source may submit information and
3 argument in opposition to the recommendation;

4 “(D) of the procedures governing the re-
5 view and possible issuance of an exclusion or re-
6 moval order pursuant to paragraph (5); and

7 “(E) where practicable, in the Council’s
8 sole and unreviewable discretion, a description
9 of mitigation steps that could be taken by the
10 source that may result in the Council rescinding
11 the recommendation.

12 “(4) CONFIDENTIALITY.—Any notice issued to
13 a source under paragraph (3) shall be kept confiden-
14 tial until—

15 “(A) an exclusion or removal order is
16 issued pursuant to paragraph (5); and

17 “(B) the source has been notified pursuant
18 to paragraph (6).

19 “(5) EXCLUSION AND REMOVAL ORDERS.—

20 “(A) ORDER ISSUANCE.—Recommendations
21 of the Council under paragraph (2), together
22 with any information submitted by a
23 source under paragraph (3) related to such a
24 recommendation, shall be reviewed by the fol-
25 lowing officials, who may issue exclusion and

1 removal orders based upon such recommenda-
2 tions:

3 “(i) The Secretary of Homeland Secu-
4 rity, for exclusion and removal orders ap-
5 plicable to civilian agencies, to the extent
6 not covered by clause (ii) or (iii).

7 “(ii) The Secretary of Defense, for ex-
8 clusion and removal orders applicable to
9 the Department of Defense and national
10 security systems other than sensitive com-
11 partmented information systems.

12 “(iii) The Director of National Intel-
13 ligence, for exclusion and removal orders
14 applicable to the intelligence community
15 and sensitive compartmented information
16 systems, to the extent not covered by
17 clause (ii).

18 “(B) DELEGATION.—The officials identi-
19 fied in subparagraph (A) may not delegate any
20 authority under this subparagraph to an official
21 below the level one level below the Deputy Sec-
22 retary or Principal Deputy Director, except that
23 the Secretary of Defense may delegate author-
24 ity for removal orders to the Commander of the
25 United States Cyber Command, who may not

1 redelegate such authority to an official below
2 the level one level below the Deputy Com-
3 mander.

4 “(C) FACILITATION OF EXCLUSION OR-
5 DERS.—If officials identified under this para-
6 graph from the Department of Homeland Secu-
7 rity, the Department of Defense, and the Office
8 of the Director of National Intelligence issue or-
9 ders collectively resulting in a governmentwide
10 exclusion, the Administrator for General Serv-
11 ices and officials at other executive agencies re-
12 sponsible for management of the Federal Sup-
13 ply Schedules, governmentwide acquisition con-
14 tracts and multi-agency contracts shall help fa-
15 cilitate implementation of such orders by re-
16 moving the covered articles or sources identified
17 in the orders from such contracts.

18 “(D) REVIEW OF EXCLUSION AND RE-
19 MOVAL ORDERS.—The officials identified under
20 this paragraph shall review all exclusion and re-
21 moval orders issued under subparagraph (A)
22 not less frequently than annually pursuant to
23 procedures established by the Council.

24 “(E) RESCISSION.—Orders issued pursu-
25 ant to subparagraph (A) may be rescinded by

1 an authorized official from the relevant issuing
2 agency.

3 “(6) NOTIFICATIONS.—Upon issuance of an ex-
4 clusion or removal order pursuant to paragraph
5 (5)(A), the official identified under that paragraph
6 who issued the order shall—

7 “(A) notify any source named in the order
8 of—

9 “(i) the exclusion or removal order;
10 and

11 “(ii) to the extent consistent with na-
12 tional security and law enforcement inter-
13 ests, information that forms the basis for
14 the order;

15 “(B) provide classified or unclassified no-
16 tice of the exclusion or removal order to the ap-
17 propriate congressional committees and leader-
18 ship; and

19 “(C) provide the exclusion or removal
20 order to the agency identified in subsection
21 (a)(3).

22 “(7) COMPLIANCE.—Executive agencies shall
23 comply with exclusion and removal orders issued
24 pursuant to paragraph (5).

1 “(d) AUTHORITY TO REQUEST INFORMATION.—The
2 Council may request such information from executive
3 agencies as is necessary for the Council to carry out its
4 functions.

5 “(e) RELATIONSHIP TO OTHER COUNCILS.—The
6 Council shall consult and coordinate, as appropriate, with
7 other relevant councils and interagency committees, in-
8 cluding the Chief Information Officers Council, the Chief
9 Acquisition Officers Council, the Federal Acquisition Reg-
10 ulatory Council, and the Committee on Foreign Invest-
11 ment in the United States, with respect to supply chain
12 risks posed by the acquisition and use of covered articles.

13 “(f) RULES OF CONSTRUCTION.—Nothing in this
14 section shall be construed—

15 “(1) to limit the authority of the Office of Fed-
16 eral Procurement Policy to carry out the responsibil-
17 ities of that Office under any other provision of law;
18 or

19 “(2) to authorize the issuance of an exclusion
20 or removal order based solely on the fact of foreign
21 ownership of a potential procurement source that is
22 otherwise qualified to enter into procurement con-
23 tracts with the Federal Government.

1 **“§ 1324. Strategic plan**

2 “(a) IN GENERAL.—Not later than 180 days after
3 the date of the enactment of the Federal Acquisition Sup-
4 ply Chain Security Act of 2018, the Council shall develop
5 a strategic plan for addressing supply chain risks posed
6 by the acquisition of covered articles and for managing
7 such risks that includes—

8 “(1) the criteria and processes required under
9 section 1323(a) of this title, including a threshold
10 and requirements for sharing relevant information
11 about such risks with all executive agencies and, as
12 appropriate, with other Federal entities and non-
13 Federal entities;

14 “(2) an identification of existing authorities for
15 addressing such risks;

16 “(3) an identification and promulgation of best
17 practices and procedures and available resources for
18 executive agencies to assess and mitigate such risks;

19 “(4) recommendations for any legislative, regu-
20 latory, or other policy changes to improve efforts to
21 address such risks;

22 “(5) recommendations for any legislative, regu-
23 latory, or other policy changes to incentivize the
24 adoption of best practices for supply chain risk man-
25 agement by the private sector;

1 “(6) an evaluation of the effect of implementing
2 new policies or procedures on existing contracts and
3 the procurement process;

4 “(7) a plan for engaging with executive agen-
5 cies, the private sector, and other nongovernmental
6 stakeholders to address such risks;

7 “(8) a plan for identification, assessment, miti-
8 gation, and vetting of supply chain risks from exist-
9 ing and prospective information and communications
10 technology made available by executive agencies to
11 other executive agencies through common contract
12 solutions, shared services, acquisition vehicles, or
13 other assisted acquisition services; and

14 “(9) plans to strengthen the capacity of all ex-
15 ecutive agencies to conduct assessments of—

16 “(A) the supply chain risk posed by the ac-
17 quisition of covered articles; and

18 “(B) compliance with the requirements of
19 this subchapter.

20 “(b) SUBMISSION TO CONGRESS.—Not later than 7
21 calendar days after completion of the strategic plan re-
22 quired by subsection (a), the Chairperson of the Council
23 shall submit the plan to the appropriate congressional
24 committees and leadership.

1 **“§ 1325. Annual report**

2 “Not later than December 31 of each year, the Chair-
3 person of the Council shall submit to the appropriate con-
4 gressional committees and leadership a report on the ac-
5 tivities of the Council during the preceding 12-month pe-
6 riod.

7 **“§ 1326. Requirements for executive agencies**

8 “(a) IN GENERAL.—The head of each executive agen-
9 cy shall be responsible for—

10 “(1) assessing the supply chain risk posed by
11 the acquisition and use of covered articles and avoid-
12 ing, mitigating, accepting, or transferring that risk,
13 as appropriate and consistent with the standards,
14 guidelines, and practices identified by the Council
15 under section 1323(a)(1); and

16 “(2) prioritizing supply chain risk assessments
17 conducted under paragraph (1) based on the criti-
18 cality of the mission, system, component, service, or
19 asset.

20 “(b) INCLUSIONS.—The responsibility for assessing
21 supply chain risk described in subsection (a) includes—

22 “(1) developing an overall supply chain risk
23 management strategy and implementation plan and
24 policies and processes to guide and govern supply
25 chain risk management activities;

1 “(2) integrating supply chain risk management
2 practices throughout the life cycle of the system,
3 component, service, or asset;

4 “(3) limiting, avoiding, mitigating, accepting, or
5 transferring any identified risk;

6 “(4) sharing relevant information with other ex-
7 ecutive agencies as determined appropriate by the
8 Council in a manner consistent with section 1323(a)
9 of this title;

10 “(5) reporting on progress and effectiveness of
11 the agency’s supply chain risk management con-
12 sistent with guidance issued by the Office of Man-
13 agement and Budget and the Council; and

14 “(6) ensuring that all relevant information, in-
15 cluding classified information, with respect to acqui-
16 sitions of covered articles that may pose a supply
17 chain risk, consistent with section 1323(a) of this
18 title, is incorporated into existing processes of the
19 agency for conducting assessments described in sub-
20 section (a) and ongoing management of acquisition
21 programs, including any identification, investigation,
22 mitigation, or remediation needs.

23 “(c) INTERAGENCY ACQUISITIONS.—

24 “(1) IN GENERAL.—Except as provided in para-
25 graph (2), in the case of an interagency acquisition,

1 subsection (a) shall be carried out by the head of the
2 executive agency whose funds are being used to pro-
3 cure the covered article.

4 “(2) ASSISTED ACQUISITIONS.—In an assisted
5 acquisition, the parties to the acquisition shall deter-
6 mine, as part of the interagency agreement gov-
7 erning the acquisition, which agency is responsible
8 for carrying out subsection (a).

9 “(3) DEFINITIONS.—In this subsection, the
10 terms ‘assisted acquisition’ and ‘interagency acqui-
11 sition’ have the meanings given those terms in section
12 2.101 of title 48, Code of Federal Regulations (or
13 any corresponding similar regulation or ruling).

14 “(d) ASSISTANCE.—The Secretary of Homeland Se-
15 curity may—

16 “(1) assist executive agencies in conducting risk
17 assessments described in subsection (a) and imple-
18 menting mitigation requirements for information
19 and communications technology; and

20 “(2) provide such additional guidance or tools
21 as are necessary to support actions taken by execu-
22 tive agencies.

23 **“§ 1327. Judicial review procedures**

24 “(a) IN GENERAL.—Except as provided in subsection
25 (b) and chapter 71 of this title, and notwithstanding any

1 other provision of law, an action taken under section 1323
2 or 4713 of this title, or any action taken by an executive
3 agency to implement such an action, shall not be subject
4 to administrative review or judicial review, including bid
5 protests before the Government Accountability Office or
6 in any Federal court.

7 “(b) PETITIONS.—

8 “(1) IN GENERAL.—Not later than 60 days
9 after a party is notified of an exclusion or removal
10 order under section 1323(c)(6) of this title or a cov-
11 ered procurement action under section 4713 of this
12 title, the party may file a petition for judicial review
13 in the United States Court of Appeals for the Dis-
14 trict of Columbia Circuit claiming that the issuance
15 of the exclusion or removal order or covered procure-
16 ment action is unlawful.

17 “(2) STANDARD OF REVIEW.—The Court shall
18 hold unlawful a covered action taken under sections
19 1323 or 4713 of this title, in response to a petition
20 that the court finds to be—

21 “(A) arbitrary, capricious, an abuse of dis-
22 cretion, or otherwise not in accordance with
23 law;

24 “(B) contrary to constitutional right,
25 power, privilege, or immunity;

1 “(C) in excess of statutory jurisdiction, au-
2 thority, or limitation, or short of statutory
3 right;

4 “(D) lacking substantial support in the ad-
5 ministrative record taken as a whole or in clas-
6 sified information submitted to the court under
7 paragraph (3); or

8 “(E) not in accord with procedures re-
9 quired by law.

10 “(3) EXCLUSIVE JURISDICTION.—The United
11 States Court of Appeals for the District of Columbia
12 Circuit shall have exclusive jurisdiction over claims
13 arising under sections 1323(c)(5) or 4713 of this
14 title against the United States, any United States
15 department or agency, or any component or official
16 of any such department or agency, subject to review
17 by the Supreme Court of the United States under
18 section 1254 of title 28.

19 “(4) ADMINISTRATIVE RECORD AND PROCE-
20 DURES.—

21 “(A) IN GENERAL.—The procedures de-
22 scribed in this paragraph shall apply to the re-
23 view of a petition under this section.

24 “(B) ADMINISTRATIVE RECORD.—

1 “(i) FILING OF RECORD.—The United
2 States shall file with the court an adminis-
3 trative record, which shall consist of the
4 information that the appropriate official
5 relied upon in issuing an exclusion or re-
6 moval order under section 1323(c)(5) or a
7 covered procurement action under section
8 4713 of this title.

9 “(ii) UNCLASSIFIED, NONPRIVILEGED
10 INFORMATION.—All unclassified informa-
11 tion contained in the administrative record
12 that is not otherwise privileged or subject
13 to statutory protections shall be provided
14 to the petitioner with appropriate protec-
15 tions for any privileged or confidential
16 trade secrets and commercial or financial
17 information.

18 “(iii) IN CAMERA AND EX PARTE.—
19 The following information may be included
20 in the administrative record and shall be
21 submitted only to the court ex parte and in
22 camera:

23 “(I) Classified information.

1 “(II) Sensitive security informa-
2 tion, as defined by section 1520.5 of
3 title 49, Code of Federal Regulations.

4 “(III) Privileged law enforcement
5 information.

6 “(IV) Information obtained or
7 derived from any activity authorized
8 under the Foreign Intelligence Sur-
9 veillance Act of 1978 (50 U.S.C. 1801
10 et seq.), except that, with respect to
11 such information, subsections (e), (e),
12 (f), (g), and (h) of section 106 (50
13 U.S.C. 1806), subsections (d), (f), (g),
14 (h), and (i) of section 305 (50 U.S.C.
15 1825), subsections (e), (e), (f), (g),
16 and (h) of section 405 (50 U.S.C.
17 1845), and section 706 (50 U.S.C.
18 1881e) of that Act shall not apply.

19 “(V) Information subject to privi-
20 lege or protections under any other
21 provision of law.

22 “(iv) UNDER SEAL.—Any information
23 that is part of the administrative record
24 filed ex parte and in camera under clause
25 (iii), or cited by the court in any decision,

1 shall be treated by the court consistent
2 with the provisions of this subparagraph
3 and shall remain under seal and preserved
4 in the records of the court to be made
5 available consistent with the above provi-
6 sions in the event of further proceedings.
7 In no event shall such information be re-
8 leased to the petitioner or as part of the
9 public record.

10 “(v) RETURN.—After the expiration
11 of the time to seek further review, or the
12 conclusion of further proceedings, the
13 court shall return the administrative
14 record, including any and all copies, to the
15 United States.

16 “(C) EXCLUSIVE REMEDY.—A determina-
17 tion by the court under this subsection shall be
18 the exclusive judicial remedy for any claim de-
19 scribed in this section against the United
20 States, any United States department or agen-
21 cy, or any component or official of any such de-
22 partment or agency.

23 “(D) RULE OF CONSTRUCTION.—Nothing
24 in this section shall be construed as limiting,
25 superseding, or preventing the invocation of,

1 any privileges or defenses that are otherwise
2 available at law or in equity to protect against
3 the disclosure of information.

4 “(c) DEFINITION.—In this section, the term ‘classi-
5 fied information’—

6 “(1) has the meaning given that term in section
7 1(a) of the Classified Information Procedures Act
8 (18 U.S.C. App.); and

9 “(2) includes—

10 “(A) any information or material that has
11 been determined by the United States Govern-
12 ment pursuant to an Executive order, statute,
13 or regulation to require protection against un-
14 authorized disclosure for reasons of national se-
15 curity; and

16 “(B) any restricted data, as defined in sec-
17 tion 11 of the Atomic Energy Act of 1954 (42
18 U.S.C. 2014).

19 **“§ 1328. Termination**

20 “This subchapter shall terminate on the date that is
21 5 years after the date of the enactment of the Federal
22 Acquisition Supply Chain Security Act of 2018.”.

23 (b) CLERICAL AMENDMENT.—The table of sections
24 at the beginning of chapter 13 of such title is amended
25 by adding at the end the following new items:

“SUBCHAPTER III—FEDERAL ACQUISITION SUPPLY CHAIN SECURITY

“Sec.

“1321. Definitions.

“1322. Federal Acquisition Security Council establishment and membership.

“1323. Functions and authorities.

“1324. Strategic plan.

“1325. Annual report.

“1326. Requirements for executive agencies.

“1327. Judicial review procedures.

“1328. Termination.”.

1 (c) EFFECTIVE DATE.—The amendments made by
2 this section shall take effect on the date that is 90 days
3 after the date of the enactment of this Act and shall apply
4 to contracts that are awarded before, on, or after that
5 date.

6 (d) IMPLEMENTATION.—

7 (1) INTERIM FINAL RULE.—Not later than one
8 year after the date of the enactment of this Act, the
9 Federal Acquisition Security Council shall prescribe
10 an interim final rule to implement subchapter III of
11 chapter 13 of title 41, United States Code, as added
12 by subsection (a).

13 (2) FINAL RULE.—Not later than one year
14 after prescribing the interim final rule under para-
15 graph (1) and considering public comments with re-
16 spect to such interim final rule, the Council shall
17 prescribe a final rule to implement subchapter III of
18 chapter 13 of title 41, United States Code, as added
19 by subsection (a).

20 (3) FAILURE TO ACT.—

1 (A) IN GENERAL.—If the Council does not
2 issue a final rule in accordance with paragraph
3 (2) on or before the last day of the one-year pe-
4 riod referred to in that paragraph, the Council
5 shall submit to the appropriate congressional
6 committees and leadership, not later than 10
7 days after such last day and every 90 days
8 thereafter until the final rule is issued, a report
9 explaining why the final rule was not timely
10 issued and providing an estimate of the earliest
11 date on which the final rule will be issued.

12 (B) APPROPRIATE CONGRESSIONAL COM-
13 MITTEES AND LEADERSHIP DEFINED.—In this
14 paragraph, the term “appropriate congressional
15 committees and leadership” has the meaning
16 given that term in section 1321 of title 41,
17 United States Code, as added by subsection (a).

18 **SEC. 203. AUTHORITIES OF EXECUTIVE AGENCIES RELAT-**
19 **ING TO MITIGATING SUPPLY CHAIN RISKS IN**
20 **THE PROCUREMENT OF COVERED ARTICLES.**

21 (a) IN GENERAL.—Chapter 47 of title 41, United
22 States Code, is amended by adding at the end the fol-
23 lowing new section:

1 **“§ 4713. Authorities relating to mitigating supply**
2 **chain risks in the procurement of cov-**
3 **ered articles**

4 “(a) AUTHORITY.—Subject to subsection (b), the
5 head of an executive agency may carry out a covered pro-
6 curement action.

7 “(b) DETERMINATION AND NOTIFICATION.—Except
8 as authorized by subsection (c) to address an urgent na-
9 tional security interest, the head of an executive agency
10 may exercise the authority provided in subsection (a) only
11 after—

12 “(1) obtaining a joint recommendation, in un-
13 classified or classified form, from the chief acquisi-
14 tion officer and the chief information officer of the
15 agency, or officials performing similar functions in
16 the case of executive agencies that do not have such
17 officials, which includes a review of any risk assess-
18 ment made available by the executive agency identi-
19 fied under section 1323(a)(3) of this title, that there
20 is a significant supply chain risk in a covered pro-
21 curement;

22 “(2) providing notice of the joint recommenda-
23 tion described in paragraph (1) to any source named
24 in the joint recommendation advising—

25 “(A) that a recommendation is being con-
26 sidered or has been obtained;

1 “(B) to the extent consistent with the na-
2 tional security and law enforcement interests, of
3 information that forms the basis for the rec-
4 ommendation;

5 “(C) that, within 30 days after receipt of
6 the notice, the source may submit information
7 and argument in opposition to the recommenda-
8 tion; and

9 “(D) of the procedures governing the con-
10 sideration of the submission and the possible
11 exercise of the authority provided in subsection
12 (a);

13 “(3) making a determination in writing, in un-
14 classified or classified form, after considering any in-
15 formation submitted by a source under paragraph
16 (2) and in consultation with the chief information
17 security officer of the agency, that—

18 “(A) use of the authority under subsection
19 (a) is necessary to protect national security by
20 reducing supply chain risk;

21 “(B) less intrusive measures are not rea-
22 sonably available to reduce such supply chain
23 risk; and

24 “(C) the use of such authorities will apply
25 to a single covered procurement or a class of

1 covered procurements, and otherwise specifies
2 the scope of the determination; and

3 “(4) providing a classified or unclassified notice
4 of the determination made under paragraph (3) to
5 the appropriate congressional committees and lead-
6 ership that includes—

7 “(A) the joint recommendation described
8 in paragraph (1);

9 “(B) a summary of any risk assessment re-
10 viewed in support of the joint recommendation
11 required by paragraph (1); and

12 “(C) a summary of the basis for the deter-
13 mination, including a discussion of less intru-
14 sive measures that were considered and why
15 such measures were not reasonably available to
16 reduce supply chain risk.

17 “(c) PROCEDURES TO ADDRESS URGENT NATIONAL
18 SECURITY INTERESTS.—In any case in which the head of
19 an executive agency determines that an urgent national
20 security interest requires the immediate exercise of the au-
21 thority provided in subsection (a), the head of the agen-
22 cy—

23 “(1) may, to the extent necessary to address
24 such national security interest, and subject to the
25 conditions in paragraph (2)—

1 “(A) temporarily delay the notice required
2 by subsection (b)(2);

3 “(B) make the determination required by
4 subsection (b)(3), regardless of whether the no-
5 tice required by subsection (b)(2) has been pro-
6 vided or whether the notified source has sub-
7 mitted any information in response to such no-
8 tice;

9 “(C) temporarily delay the notice required
10 by subsection (b)(4); and

11 “(D) exercise the authority provided in
12 subsection (a) in accordance with such deter-
13 mination within 60 calendar days after the day
14 the determination is made; and

15 “(2) shall take actions necessary to comply with
16 all requirements of subsection (b) as soon as prac-
17 ticable after addressing the urgent national security
18 interest, including—

19 “(A) providing the notice required by sub-
20 section (b)(2);

21 “(B) promptly considering any information
22 submitted by the source in response to such no-
23 tice, and making any appropriate modifications
24 to the determination based on such information;

1 “(C) providing the notice required by sub-
2 section (b)(4), including a description of the ur-
3 gent national security interest, and any modi-
4 fications to the determination made in accord-
5 ance with subparagraph (B); and

6 “(D) providing notice to the appropriate
7 congressional committees and leadership within
8 7 calendar days of the covered procurement ac-
9 tions taken under this section.

10 “(d) CONFIDENTIALITY.—The notice required by
11 subsection (b)(2) shall be kept confidential until a deter-
12 mination with respect to a covered procurement action has
13 been made pursuant to subsection (b)(3).

14 “(e) DELEGATION.—The head of an executive agency
15 may not delegate the authority provided in subsection (a)
16 or the responsibility identified in subsection (f) to an offi-
17 cial below the level one level below the Deputy Secretary
18 or Principal Deputy Director.

19 “(f) ANNUAL REVIEW OF DETERMINATIONS.—The
20 head of an executive agency shall conduct an annual re-
21 view of all determinations made by such head under sub-
22 section (b) and promptly amend any covered procurement
23 action as appropriate.

1 “(g) REGULATIONS.—The Federal Acquisition Regu-
2 latory Council shall prescribe such regulations as may be
3 necessary to carry out this section.

4 “(h) REPORTS REQUIRED.—Not less frequently than
5 annually, the head of each executive agency that exercised
6 the authority provided in subsection (a) or (c) during the
7 preceding 12-month period shall submit to the appropriate
8 congressional committees and leadership a report summa-
9 rizing the actions taken by the agency under this section
10 during that 12-month period.

11 “(i) RULE OF CONSTRUCTION.—Nothing in this sec-
12 tion shall be construed to authorize the head of an execu-
13 tive agency to carry out a covered procurement action
14 based solely on the fact of foreign ownership of a potential
15 procurement source that is otherwise qualified to enter
16 into procurement contracts with the Federal Government.

17 “(j) TERMINATION.—The authority provided under
18 subsection (a) shall terminate on the date that is 5 years
19 after the date of the enactment of the Federal Acquisition
20 Supply Chain Security Act of 2018.

21 “(k) DEFINITIONS.—In this section:

22 “(1) APPROPRIATE CONGRESSIONAL COMMIT-
23 TEES AND LEADERSHIP.—The term ‘appropriate
24 congressional committees and leadership’ means—

1 “(A) the Committee on Homeland Security
2 and Governmental Affairs, the Committee on
3 the Judiciary, the Committee on Appropria-
4 tions, the Committee on Armed Services, the
5 Committee on Commerce, Science, and Trans-
6 portation, the Select Committee on Intelligence,
7 and the majority and minority leader of the
8 Senate; and

9 “(B) the Committee on Oversight and Gov-
10 ernment Reform, the Committee on the Judici-
11 ary, the Committee on Appropriations, the
12 Committee on Homeland Security, the Com-
13 mittee on Armed Services, the Committee on
14 Energy and Commerce, the Permanent Select
15 Committee on Intelligence, and the Speaker and
16 minority leader of the House of Representa-
17 tives.

18 “(2) COVERED ARTICLE.—The term ‘covered
19 article’ means—

20 “(A) information technology, as defined in
21 section 11101 of title 40, including cloud com-
22 puting services of all types;

23 “(B) telecommunications equipment or
24 telecommunications service, as those terms are

1 defined in section 3 of the Communications Act
2 of 1934 (47 U.S.C. 153);

3 “(C) the processing of information on a
4 Federal or non-Federal information system,
5 subject to the requirements of the Controlled
6 Unclassified Information program; or

7 “(D) hardware, systems, devices, software,
8 or services that include embedded or incidental
9 information technology.

10 “(3) COVERED PROCUREMENT.—The term ‘cov-
11 ered procurement’ means—

12 “(A) a source selection for a covered arti-
13 cle involving either a performance specification,
14 as provided in subsection (a)(3)(B) of section
15 3306 of this title, or an evaluation factor, as
16 provided in subsection (b)(1)(A) of such section,
17 relating to a supply chain risk, or where supply
18 chain risk considerations are included in the
19 agency’s determination of whether a source is a
20 responsible source as defined in section 113 of
21 this title;

22 “(B) the consideration of proposals for and
23 issuance of a task or delivery order for a cov-
24 ered article, as provided in section 4106(d)(3)
25 of this title, where the task or delivery order

1 contract includes a contract clause establishing
2 a requirement relating to a supply chain risk;

3 “(C) any contract action involving a con-
4 tract for a covered article where the contract in-
5 cludes a clause establishing requirements relat-
6 ing to a supply chain risk; or

7 “(D) any other procurement in a category
8 of procurements determined appropriate by the
9 Federal Acquisition Regulatory Council, with
10 the advice of the Federal Acquisition Security
11 Council.

12 “(4) COVERED PROCUREMENT ACTION.—The
13 term ‘covered procurement action’ means any of the
14 following actions, if the action takes place in the
15 course of conducting a covered procurement:

16 “(A) The exclusion of a source that fails to
17 meet qualification requirements established
18 under section 3311 of this title for the purpose
19 of reducing supply chain risk in the acquisition
20 or use of covered articles.

21 “(B) The exclusion of a source that fails to
22 achieve an acceptable rating with regard to an
23 evaluation factor providing for the consideration
24 of supply chain risk in the evaluation of pro-

1 posals for the award of a contract or the
2 issuance of a task or delivery order.

3 “(C) The determination that a source is
4 not a responsible source as defined in section
5 113 of this title based on considerations of sup-
6 ply chain risk.

7 “(D) The decision to withhold consent for
8 a contractor to subcontract with a particular
9 source or to direct a contractor to exclude a
10 particular source from consideration for a sub-
11 contract under the contract.

12 “(5) INFORMATION AND COMMUNICATIONS
13 TECHNOLOGY.—The term ‘information and commu-
14 nications technology’ means—

15 “(A) information technology, as defined in
16 section 11101 of title 40;

17 “(B) information systems, as defined in
18 section 3502 of title 44; and

19 “(C) telecommunications equipment and
20 telecommunications services, as those terms are
21 defined in section 3 of the Communications Act
22 of 1934 (47 U.S.C. 153).

23 “(6) SUPPLY CHAIN RISK.—The term ‘supply
24 chain risk’ means the risk that any person may sab-
25 otage, maliciously introduce unwanted function, ex-

1 tract data, or otherwise manipulate the design, in-
 2 tegrity, manufacturing, production, distribution, in-
 3 stallation, operation, maintenance, disposition, or re-
 4 tirement of covered articles so as to surveil, deny,
 5 disrupt, or otherwise manipulate the function, use,
 6 or operation of the covered articles or information
 7 stored or transmitted on the covered articles.

8 “(7) EXECUTIVE AGENCY.—Notwithstanding
 9 section 3101(c)(1), this section applies to the De-
 10 partment of Defense, the Coast Guard, and the Na-
 11 tional Aeronautics and Space Administration.”.

12 (b) CLERICAL AMENDMENT.—The table of sections
 13 at the beginning of chapter 47 of such title is amended
 14 by adding at the end the following new item:

“4713. Authorities relating to mitigating supply chain risks in the procurement
 of covered articles.”.

15 (c) EFFECTIVE DATE.—The amendments made by
 16 this section shall take effect on the date that is 90 days
 17 after the date of the enactment of this Act and shall apply
 18 to contracts that are awarded before, on, or after that
 19 date.

20 **SEC. 204. FEDERAL INFORMATION SECURITY MODERNIZA-**
 21 **TION ACT.**

22 (a) IN GENERAL.—Title 44, United States Code, is
 23 amended—

1 (1) in section 3553(a)(5), by inserting “and
2 section 1326 of title 41” after “compliance with the
3 requirements of this subchapter”; and

4 (2) in section 3554(a)(1)(B)—

5 (A) by inserting “, subchapter III of chap-
6 ter 13 of title 41,” after “complying with the
7 requirements of this subchapter”;

8 (B) in clause (iv), by striking “; and” and
9 inserting a semicolon; and

10 (C) by adding at the end the following new
11 clause:

12 “(vi) responsibilities relating to as-
13 sessing and avoiding, mitigating, transfer-
14 ring, or accepting supply chain risks under
15 section 1326 of title 41, and complying
16 with exclusion and removal orders issued
17 under section 1323 of such title; and”.

18 (b) **RULE OF CONSTRUCTION.**—Nothing in this title
19 shall be construed to alter or impede any authority or re-
20 sponsibility under section 3553 of title 44, United States
21 Code.

22 **SEC. 205. EFFECTIVE DATE.**

23 This title shall take effect on the date that is 90 days
24 after the date of the enactment of this Act.