

115TH CONGRESS  
2D SESSION

# H. R. 7327

---

## AN ACT

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-  
 6       lizing Risk Exposure Technology Act” or the “SECURE  
 7       Technology Act”.

8       (b) **TABLE OF CONTENTS.**—The table of contents for  
 9       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.

10       **TITLE       I—DEPARTMENT       OF**  
 11       **HOMELAND SECURITY INFOR-**  
 12       **MATION       SECURITY       AND**  
 13       **OTHER MATTERS**

14       **SEC. 101. DEPARTMENT OF HOMELAND SECURITY DISCLO-**  
 15       **SURE OF SECURITY VULNERABILITIES.**

16       (a) **VULNERABILITY DISCLOSURE POLICY.**—The Sec-  
 17       retary of Homeland Security shall establish a policy appli-

1 cable to individuals, organizations, and companies that re-  
2 port security vulnerabilities on appropriate information  
3 systems of Department of Homeland Security. Such policy  
4 shall include each of the following:

5 (1) The appropriate information systems of the  
6 Department that individuals, organizations, and  
7 companies may use to discover and report security  
8 vulnerabilities on appropriate information systems.

9 (2) The conditions and criteria under which in-  
10 dividuals, organizations, and companies may operate  
11 to discover and report security vulnerabilities.

12 (3) How individuals, organizations, and compa-  
13 nies may disclose to the Department security  
14 vulnerabilities discovered on appropriate information  
15 systems of the Department.

16 (4) The ways in which the Department may  
17 communicate with individuals, organizations, and  
18 companies that report security vulnerabilities.

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

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

1 (c) CONSULTATION.—

2 (1) IN GENERAL.—In developing the security  
3 vulnerability disclosure policy under subsection (a),  
4 the Secretary of Homeland Security shall consult  
5 with each of the following:

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

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

18 (C) Non-governmental security researchers.

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

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

25 (e) SUBMISSION TO CONGRESS.—

1           (1) DISCLOSURE POLICY AND REMEDIATION  
2           PROCESS.—Not later than 90 days after the date of  
3           the enactment of this Act, the Secretary of Home-  
4           land Security shall submit to the appropriate con-  
5           gressional committees a copy of the policy required  
6           under subsection (a) and the remediation process re-  
7           quired under subsection (b).

8           (2) REPORT AND BRIEFING.—

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

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

24          (C) MATTERS FOR INCLUSION.—The re-  
25          port required under subparagraph (A) and the

1 briefings required under subparagraph (B) shall  
2 include each of the following with respect to the  
3 policy required under subsection (a) and the  
4 process required under subsection (b) for the  
5 period covered by the report or briefing, as the  
6 case may be:

7 (i) The number of unique security  
8 vulnerabilities reported.

9 (ii) The number of previously un-  
10 known security vulnerabilities mitigated or  
11 remediated.

12 (iii) The number of unique individ-  
13 uals, organizations, and companies that re-  
14 ported security vulnerabilities.

15 (iv) The average length of time be-  
16 tween the reporting of security  
17 vulnerabilities and mitigation or remedi-  
18 ation of such vulnerabilities.

19 (f) DEFINITIONS.—In this section:

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

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

4           (3) The term “appropriate information system”  
5           means an information system that the Secretary of  
6           Homeland Security selects for inclusion under the  
7           vulnerability disclosure policy required by subsection  
8           (a).

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

11                (A) the Committee on Homeland Security,  
12                the Committee on Armed Services, the Com-  
13                mittee on Energy and Commerce, and the Per-  
14                manent Select Committee on Intelligence of the  
15                House of Representatives; and

16                (B) the Committee on Homeland Security  
17                and Governmental Affairs, the Committee on  
18                Armed Services, the Committee on Commerce,  
19                Science, and Transportation, and the Select  
20                Committee on Intelligence of the Senate.

21 **SEC. 102. DEPARTMENT OF HOMELAND SECURITY BUG**  
22 **BOUNTY PILOT PROGRAM.**

23           (a) DEFINITIONS.—In this section:

24                (1) The term “appropriate congressional com-  
25                mittees” means—

1 (A) the Committee on Homeland Security  
2 and Governmental Affairs of the Senate;

3 (B) the Select Committee on Intelligence  
4 of the Senate;

5 (C) the Committee on Homeland Security  
6 of the House of Representatives; and

7 (D) Permanent Select Committee on Intel-  
8 ligence of the House of Representatives.

9 (2) The term “bug bounty program” means a  
10 program under which—

11 (A) individuals, organizations, and compa-  
12 nies are temporarily authorized to identify and  
13 report vulnerabilities of appropriate information  
14 systems of the Department; and

15 (B) eligible individuals, organizations, and  
16 companies receive compensation in exchange for  
17 such reports.

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

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



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

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

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

9           (b) BUG BOUNTY PILOT PROGRAM.—

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

16           (2) RESPONSIBILITIES OF SECRETARY.—In es-  
17           tablishing and conducting the pilot program, the  
18           Secretary shall—

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

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

1 (C) establish criteria for individuals, orga-  
2 nizations, and companies to be considered eligi-  
3 ble for compensation under the pilot program in  
4 compliance with Federal laws;

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

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

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

1 (G) engage qualified interested persons, in-  
2 cluding non-government sector representatives,  
3 about the structure of the pilot program as con-  
4 structive and to the extent practicable.

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

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

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

19 (A) registered;

20 (B) were determined eligible;

21 (C) submitted security vulnerabilities; and

22 (D) received compensation;

23 (2) the number and severity of vulnerabilities  
24 reported as part of the pilot program;

1           (3) the number of previously unidentified secu-  
2       rity vulnerabilities remediated as a result of the pilot  
3       program;

4           (4) the current number of outstanding pre-  
5       viously unidentified security vulnerabilities and De-  
6       partment remediation plans;

7           (5) the average length of time between the re-  
8       porting of security vulnerabilities and remediation of  
9       the vulnerabilities;

10          (6) the types of compensation provided under  
11       the pilot program; and

12          (7) the lessons learned from the pilot program.

13       (d) AUTHORIZATION OF APPROPRIATIONS.—There is  
14       authorized to be appropriated to the Department  
15       \$250,000 for fiscal year 2019 to carry out this section.

16       **SEC. 103. CONGRESSIONAL SUBMITTAL OF REPORTS RE-**  
17                               **LATING TO CERTAIN SPECIAL ACCESS PRO-**  
18                               **GRAMS AND SIMILAR PROGRAMS.**

19       The National Defense Authorization Act for Fiscal  
20       Year 1994 (50 U.S.C. 3348) is amended—

21           (1) by striking “Congress” each place it ap-  
22       pears and inserting “the congressional oversight  
23       committees”;

1           (2) in subsection (f)(1), by striking “appro-  
2       pate oversight committees” and inserting “congres-  
3       sional oversight committees”; and

4           (3) in subsection (g)—

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

7                 (B) by inserting before paragraph (2), as  
8       so redesignated, the following:

9           “(1) CONGRESSIONAL OVERSIGHT COMMIT-  
10       TEES.—The term ‘congressional oversight commit-  
11       tees’ means—

12                 “(A) congressional leadership and author-  
13       izing and appropriations congressional commit-  
14       tees with jurisdiction or shared jurisdiction over  
15       a department or agency;

16                 “(B) the Committee on Homeland Security  
17       and Governmental Affairs of the Senate; and

18                 “(C) the Committee on Oversight and Gov-  
19       ernment Reform of the House of Representa-  
20       tives.”.

1 **TITLE II—FEDERAL ACQUISITION**  
2 **TION SUPPLY CHAIN SECURITY**  
3 **RITY**

4 **SEC. 201. SHORT TITLE.**

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

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

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

11 “SUBCHAPTER III—FEDERAL ACQUISITION  
12 SUPPLY CHAIN SECURITY

13 “§ 1321. Definitions

14 “In this subchapter:

15 “(1) APPROPRIATE CONGRESSIONAL COMMIT-  
16 TEES AND LEADERSHIP.—The term ‘appropriate  
17 congressional committees and leadership’ means—

18 “(A) the Committee on Homeland Security  
19 and Governmental Affairs, the Committee on  
20 the Judiciary, the Committee on Appropria-  
21 tions, the Committee on Armed Services, the  
22 Committee on Commerce, Science, and Trans-  
23 portation, the Select Committee on Intelligence,  
24 and the majority and minority leader of the  
25 Senate; and

1 “(B) the Committee on Oversight and Gov-  
2 ernment Reform, the Committee on the Judici-  
3 ary, the Committee on Appropriations, the  
4 Committee on Homeland Security, the Com-  
5 mittee on Armed Services, the Committee on  
6 Energy and Commerce, the Permanent Select  
7 Committee on Intelligence, and the Speaker and  
8 minority leader of the House of Representa-  
9 tives.

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

13 “(3) COVERED ARTICLE.—The term ‘covered  
14 article’ has the meaning given that term in section  
15 4713 of this title.

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

19 “(5) INFORMATION AND COMMUNICATIONS  
20 TECHNOLOGY.—The term ‘information and commu-  
21 nications technology’ has the meaning given that  
22 term in section 4713 of this title.

23 “(6) INTELLIGENCE COMMUNITY.—The term  
24 ‘intelligence community’ has the meaning given that

1 term in section 3(4) of the National Security Act of  
2 1947 (50 U.S.C. 3003(4)).

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

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

9 **“§ 1322. Federal Acquisition Security Council estab-**  
10 **lishment and membership**

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

13 “(b) MEMBERSHIP.—

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

16 “(A) The Office of Management and  
17 Budget.

18 “(B) The General Services Administration.

19 “(C) The Department of Homeland Secu-  
20 rity, including the Cybersecurity and Infra-  
21 structure Security Agency.

22 “(D) The Office of the Director of Na-  
23 tional Intelligence, including the National Coun-  
24 terintelligence and Security Center.



1           “(E) The Department of Justice, including  
2           the Federal Bureau of Investigation.

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

5           “(G) The Department of Commerce, in-  
6           cluding the National Institute of Standards and  
7           Technology.

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

10          “(2) LEAD REPRESENTATIVES.—

11                 “(A) DESIGNATION.—

12                         “(i) IN GENERAL.—Not later than 45  
13                         days after the date of the enactment of the  
14                         Federal Acquisition Supply Chain Security  
15                         Act of 2018, the head of each agency rep-  
16                         resented on the Council shall designate a  
17                         representative of that agency as the lead  
18                         representative of the agency on the Coun-  
19                         cil.

20                         “(ii) REQUIREMENTS.—The rep-  
21                         resentative of an agency designated under  
22                         clause (i) shall have expertise in supply  
23                         chain risk management, acquisitions, or in-  
24                         formation and communications technology.

1           “(B) FUNCTIONS.—The lead representa-  
2           tive of an agency designated under subpara-  
3           graph (A) shall ensure that appropriate per-  
4           sonnel, including leadership and subject matter  
5           experts of the agency, are aware of the business  
6           of the Council.

7           “(c) CHAIRPERSON.—

8           “(1) DESIGNATION.—Not later than 45 days  
9           after the date of the enactment of the Federal Ac-  
10          quisition Supply Chain Security Act of 2018, the Di-  
11          rector of the Office of Management and Budget  
12          shall designate a senior-level official from the Office  
13          of Management and Budget to serve as the Chair-  
14          person of the Council.

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

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

19               “(B) designating executive agencies to be  
20               represented on the Council under subsection  
21               (b)(1)(H);

22               “(C) in consultation with the lead rep-  
23               resentative of each agency represented on the  
24               Council, developing a charter for the Council;  
25               and

1           “(D) not later than 7 days after comple-  
2           tion of the charter, submitting the charter to  
3           the appropriate congressional committees and  
4           leadership.

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

9           **“§ 1323. Functions and authorities**

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

12               “(1) Identifying and recommending develop-  
13               ment by the National Institute of Standards and  
14               Technology of supply chain risk management stand-  
15               ards, guidelines, and practices for executive agencies  
16               to use when assessing and developing mitigation  
17               strategies to address supply chain risks, particularly  
18               in the acquisition and use of covered articles under  
19               section 1326(a) of this title.

20               “(2) Identifying or developing criteria for shar-  
21               ing information with executive agencies, other Fed-  
22               eral entities, and non-Federal entities with respect to  
23               supply chain risk, including information related to  
24               the exercise of authorities provided under this sec-

tion and sections 1326 and 4713 of this title. At a minimum, such criteria shall address—

“(A) the content to be shared;

“(B) the circumstances under which sharing is mandated or voluntary; and

“(C) the circumstances under which it is appropriate for an executive agency to rely on information made available through such sharing in exercising the responsibilities and authorities provided under this section and section 4713 of this title.

“(3) Identifying an appropriate executive agency to—

“(A) accept information submitted by executive agencies based on the criteria established under paragraph (2);

“(B) facilitate the sharing of information received under subparagraph (A) to support supply chain risk analyses under section 1326 of this title, recommendations under this section, and covered procurement actions under section 4713 of this title;

“(C) share with the Council information regarding covered procurement actions by exec-

1           utive agencies taken under section 4713 of this  
2           title; and

3                 “(D) inform the Council of orders issued  
4           under this section.

5                 “(4) Identifying, as appropriate, executive agen-  
6           cies to provide—

7                         “(A) shared services, such as support for  
8           making risk assessments, validation of products  
9           that may be suitable for acquisition, and miti-  
10          gation activities; and

11                        “(B) common contract solutions to support  
12          supply chain risk management activities, such  
13          as subscription services or machine-learning-en-  
14          hanced analysis applications to support in-  
15          formed decision making.

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

21                 “(6) Engaging with the private sector and other  
22          nongovernmental stakeholders in performing the  
23          functions described in paragraphs (1) and (2) and  
24          on issues relating to the management of supply

1 chain risks posed by the acquisition of covered arti-  
2 cles.

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

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

12 “(c) AUTHORITY FOR EXCLUSION OR REMOVAL OR-  
13 DERS.—

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

17 “(A) recommending orders applicable to  
18 executive agencies requiring the exclusion of  
19 sources or covered articles from executive agen-  
20 cy procurement actions (in this section referred  
21 to as ‘exclusion orders’);

22 “(B) recommending orders applicable to  
23 executive agencies requiring the removal of cov-  
24 ered articles from executive agency information

1 systems (in this section referred to as ‘removal  
2 orders’);

3 “(C) requesting and approving exceptions  
4 to an issued exclusion or removal order when  
5 warranted by circumstances, including alter-  
6 native mitigation actions or other findings relat-  
7 ing to the national interest, including national  
8 security reviews, national security investiga-  
9 tions, or national security agreements; and

10 “(D) ensuring that recommended orders do  
11 not conflict with standards and guidelines  
12 issued under section 11331 of title 40 and that  
13 the Council consults with the Director of the  
14 National Institute of Standards and Technology  
15 regarding any recommended orders that would  
16 implement standards and guidelines developed  
17 by the National Institute of Standards and  
18 Technology.

19 “(2) RECOMMENDATIONS.—The Council shall  
20 use the criteria established under paragraph (1), in-  
21 formation made available under subsection (a)(3),  
22 and any other information the Council determines  
23 appropriate to issue recommendations, for applica-  
24 tion to executive agencies or any subset thereof, re-  
25 garding the exclusion of sources or covered articles

1 from any executive agency procurement action, in-  
2 cluding source selection and consent for a contractor  
3 to subcontract, or the removal of covered articles  
4 from executive agency information systems. Such  
5 recommendations shall include—

6 “(A) information necessary to positively  
7 identify the sources or covered articles rec-  
8 ommended for exclusion or removal;

9 “(B) information regarding the scope and  
10 applicability of the recommended exclusion or  
11 removal order;

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

15 “(D) a summary of the basis for the rec-  
16 ommendation, including a discussion of less in-  
17 trusive measures that were considered and why  
18 such measures were not reasonably available to  
19 reduce supply chain risk;

20 “(E) a description of the actions necessary  
21 to implement the recommended exclusion or re-  
22 moval order; and

23 “(F) where practicable, in the Council’s  
24 sole and unreviewable discretion, a description  
25 of mitigation steps that could be taken by the



1 source that may result in the Council rescinding  
2 a recommendation.

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

7 “(A) that a recommendation has been  
8 made;

9 “(B) of the criteria the Council relied upon  
10 under paragraph (1) and, to the extent con-  
11 sistent with national security and law enforce-  
12 ment interests, of information that forms the  
13 basis for the recommendation;

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

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

20 “(E) where practicable, in the Council’s  
21 sole and unreviewable discretion, a description  
22 of mitigation steps that could be taken by the  
23 source that may result in the Council rescinding  
24 the recommendation.

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

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

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

8           “(5) EXCLUSION AND REMOVAL ORDERS.—

9                   “(A) ORDER ISSUANCE.—Recommendations of the Council under paragraph (2), together with any information submitted by a source under paragraph (3) related to such a recommendation, shall be reviewed by the following officials, who may issue exclusion and removal orders based upon such recommendations:  
16                   

17                           “(i) The Secretary of Homeland Security, for exclusion and removal orders applicable to civilian agencies, to the extent not covered by clause (ii) or (iii).

21                           “(ii) The Secretary of Defense, for exclusion and removal orders applicable to the Department of Defense and national security systems other than sensitive compartmented information systems.

1                   “(iii) The Director of National Intel-  
2                   ligence, for exclusion and removal orders  
3                   applicable to the intelligence community  
4                   and sensitive compartmented information  
5                   systems, to the extent not covered by  
6                   clause (ii).

7                   “(B) DELEGATION.—The officials identi-  
8                   fied in subparagraph (A) may not delegate any  
9                   authority under this subparagraph to an official  
10                  below the level one level below the Deputy Sec-  
11                  retary or Principal Deputy Director, except that  
12                  the Secretary of Defense may delegate author-  
13                  ity for removal orders to the Commander of the  
14                  United States Cyber Command, who may not  
15                  redelegate such authority to an official below  
16                  the level one level below the Deputy Com-  
17                  mander.

18                  “(C) FACILITATION OF EXCLUSION OR-  
19                  DERS.—If officials identified under this para-  
20                  graph from the Department of Homeland Secu-  
21                  rity, the Department of Defense, and the Office  
22                  of the Director of National Intelligence issue or-  
23                  ders collectively resulting in a governmentwide  
24                  exclusion, the Administrator for General Serv-  
25                  ices and officials at other executive agencies re-

1           sponsible for management of the Federal Sup-  
2           ply Schedules, governmentwide acquisition con-  
3           tracts and multi-agency contracts shall help fa-  
4           cilitate implementation of such orders by re-  
5           moving the covered articles or sources identified  
6           in the orders from such contracts.

7           “(D) REVIEW OF EXCLUSION AND RE-  
8           MOVAL ORDERS.—The officials identified under  
9           this paragraph shall review all exclusion and re-  
10          moval orders issued under subparagraph (A)  
11          not less frequently than annually pursuant to  
12          procedures established by the Council.

13          “(E) RESCISSION.—Orders issued pursu-  
14          ant to subparagraph (A) may be rescinded by  
15          an authorized official from the relevant issuing  
16          agency.

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

21                  “(A) notify any source named in the order  
22                  of—

23                          “(i) the exclusion or removal order;  
24                          and

1                   “(ii) to the extent consistent with na-  
2                   tional security and law enforcement inter-  
3                   ests, information that forms the basis for  
4                   the order;

5                   “(B) provide classified or unclassified no-  
6                   tice of the exclusion or removal order to the ap-  
7                   propriate congressional committees and leader-  
8                   ship; and

9                   “(C) provide the exclusion or removal  
10                  order to the agency identified in subsection  
11                  (a)(3).

12                  “(7) COMPLIANCE.—Executive agencies shall  
13                  comply with exclusion and removal orders issued  
14                  pursuant to paragraph (5).

15                  “(d) AUTHORITY TO REQUEST INFORMATION.—The  
16                  Council may request such information from executive  
17                  agencies as is necessary for the Council to carry out its  
18                  functions.

19                  “(e) RELATIONSHIP TO OTHER COUNCILS.—The  
20                  Council shall consult and coordinate, as appropriate, with  
21                  other relevant councils and interagency committees, in-  
22                  cluding the Chief Information Officers Council, the Chief  
23                  Acquisition Officers Council, the Federal Acquisition Reg-  
24                  ulatory Council, and the Committee on Foreign Invest-

1 ment in the United States, with respect to supply chain  
2 risks posed by the acquisition and use of covered articles.

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

5 “(1) to limit the authority of the Office of Fed-  
6 eral Procurement Policy to carry out the responsibil-  
7 ities of that Office under any other provision of law;  
8 or

9 “(2) to authorize the issuance of an exclusion  
10 or removal order based solely on the fact of foreign  
11 ownership of a potential procurement source that is  
12 otherwise qualified to enter into procurement con-  
13 tracts with the Federal Government.

14 **“§ 1324. Strategic plan**

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

21 “(1) the criteria and processes required under  
22 section 1323(a) of this title, including a threshold  
23 and requirements for sharing relevant information  
24 about such risks with all executive agencies and, as

1 appropriate, with other Federal entities and non-  
2 Federal entities;

3 “(2) an identification of existing authorities for  
4 addressing such risks;

5 “(3) an identification and promulgation of best  
6 practices and procedures and available resources for  
7 executive agencies to assess and mitigate such risks;

8 “(4) recommendations for any legislative, regu-  
9 latory, or other policy changes to improve efforts to  
10 address such risks;

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

15 “(6) an evaluation of the effect of implementing  
16 new policies or procedures on existing contracts and  
17 the procurement process;

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

21 “(8) a plan for identification, assessment, miti-  
22 gation, and vetting of supply chain risks from exist-  
23 ing and prospective information and communications  
24 technology made available by executive agencies to  
25 other executive agencies through common contract

1 solutions, shared services, acquisition vehicles, or  
 2 other assisted acquisition services; and

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

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

7 “(B) compliance with the requirements of  
 8 this subchapter.

9 “(b) SUBMISSION TO CONGRESS.—Not later than 7  
 10 calendar days after completion of the strategic plan re-  
 11 quired by subsection (a), the Chairperson of the Council  
 12 shall submit the plan to the appropriate congressional  
 13 committees and leadership.

14 **“§ 1325. Annual report**

15 “Not later than December 31 of each year, the Chair-  
 16 person of the Council shall submit to the appropriate con-  
 17 gressional committees and leadership a report on the ac-  
 18 tivities of the Council during the preceding 12-month pe-  
 19 riod.

20 **“§ 1326. Requirements for executive agencies**

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

23 “(1) assessing the supply chain risk posed by  
 24 the acquisition and use of covered articles and avoid-  
 25 ing, mitigating, accepting, or transferring that risk,



1 as appropriate and consistent with the standards,  
2 guidelines, and practices identified by the Council  
3 under section 1323(a)(1); and

4 “(2) prioritizing supply chain risk assessments  
5 conducted under paragraph (1) based on the criti-  
6 cality of the mission, system, component, service, or  
7 asset.

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

10 “(1) developing an overall supply chain risk  
11 management strategy and implementation plan and  
12 policies and processes to guide and govern supply  
13 chain risk management activities;

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

17 “(3) limiting, avoiding, mitigating, accepting, or  
18 transferring any identified risk;

19 “(4) sharing relevant information with other ex-  
20 ecutive agencies as determined appropriate by the  
21 Council in a manner consistent with section 1323(a)  
22 of this title;

23 “(5) reporting on progress and effectiveness of  
24 the agency’s supply chain risk management con-

1       sistent with guidance issued by the Office of Man-  
2       agement and Budget and the Council; and

3           “(6) ensuring that all relevant information, in-  
4       cluding classified information, with respect to acqui-  
5       sitions of covered articles that may pose a supply  
6       chain risk, consistent with section 1323(a) of this  
7       title, is incorporated into existing processes of the  
8       agency for conducting assessments described in sub-  
9       section (a) and ongoing management of acquisition  
10      programs, including any identification, investigation,  
11      mitigation, or remediation needs.

12      “(c) INTERAGENCY ACQUISITIONS.—

13           “(1) IN GENERAL.—Except as provided in para-  
14      graph (2), in the case of an interagency acquisition,  
15      subsection (a) shall be carried out by the head of the  
16      executive agency whose funds are being used to pro-  
17      cure the covered article.

18           “(2) ASSISTED ACQUISITIONS.—In an assisted  
19      acquisition, the parties to the acquisition shall deter-  
20      mine, as part of the interagency agreement gov-  
21      erning the acquisition, which agency is responsible  
22      for carrying out subsection (a).

23           “(3) DEFINITIONS.—In this subsection, the  
24      terms ‘assisted acquisition’ and ‘interagency acquisi-  
25      tion’ have the meanings given those terms in section

1       2.101 of title 48, Code of Federal Regulations (or  
2       any corresponding similar regulation or ruling).

3       “(d) ASSISTANCE.—The Secretary of Homeland Se-  
4       curity may—

5               “(1) assist executive agencies in conducting risk  
6       assessments described in subsection (a) and imple-  
7       menting mitigation requirements for information  
8       and communications technology; and

9               “(2) provide such additional guidance or tools  
10      as are necessary to support actions taken by execu-  
11      tive agencies.

12   **“§ 1327. Judicial review procedures**

13       “(a) IN GENERAL.—Except as provided in subsection  
14   (b) and chapter 71 of this title, and notwithstanding any  
15   other provision of law, an action taken under section 1323  
16   or 4713 of this title, or any action taken by an executive  
17   agency to implement such an action, shall not be subject  
18   to administrative review or judicial review, including bid  
19   protests before the Government Accountability Office or  
20   in any Federal court.

21       “(b) PETITIONS.—

22               “(1) IN GENERAL.—Not later than 60 days  
23      after a party is notified of an exclusion or removal  
24      order under section 1323(c)(6) of this title or a cov-  
25      ered procurement action under section 4713 of this

1 title, the party may file a petition for judicial review  
2 in the United States Court of Appeals for the Dis-  
3 trict of Columbia Circuit claiming that the issuance  
4 of the exclusion or removal order or covered procure-  
5 ment action is unlawful.

6 “(2) STANDARD OF REVIEW.—The Court shall  
7 hold unlawful a covered action taken under sections  
8 1323 or 4713 of this title, in response to a petition  
9 that the court finds to be—

10 “(A) arbitrary, capricious, an abuse of dis-  
11 cretion, or otherwise not in accordance with  
12 law;

13 “(B) contrary to constitutional right,  
14 power, privilege, or immunity;

15 “(C) in excess of statutory jurisdiction, au-  
16 thority, or limitation, or short of statutory  
17 right;

18 “(D) lacking substantial support in the ad-  
19 ministrative record taken as a whole or in clas-  
20 sified information submitted to the court under  
21 paragraph (3); or

22 “(E) not in accord with procedures re-  
23 quired by law.

24 “(3) EXCLUSIVE JURISDICTION.—The United  
25 States Court of Appeals for the District of Columbia

1 Circuit shall have exclusive jurisdiction over claims  
2 arising under sections 1323(c)(5) or 4713 of this  
3 title against the United States, any United States  
4 department or agency, or any component or official  
5 of any such department or agency, subject to review  
6 by the Supreme Court of the United States under  
7 section 1254 of title 28.

8 “(4) ADMINISTRATIVE RECORD AND PROCE-  
9 DURES.—

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

13 “(B) ADMINISTRATIVE RECORD.—

14 “(i) FILING OF RECORD.—The United  
15 States shall file with the court an adminis-  
16 trative record, which shall consist of the  
17 information that the appropriate official  
18 relied upon in issuing an exclusion or re-  
19 moval order under section 1323(c)(5) or a  
20 covered procurement action under section  
21 4713 of this title.

22 “(ii) UNCLASSIFIED, NONPRIVILEGED  
23 INFORMATION.—All unclassified informa-  
24 tion contained in the administrative record  
25 that is not otherwise privileged or subject

1 to statutory protections shall be provided  
2 to the petitioner with appropriate protec-  
3 tions for any privileged or confidential  
4 trade secrets and commercial or financial  
5 information.

6 “(iii) IN CAMERA AND EX PARTE.—  
7 The following information may be included  
8 in the administrative record and shall be  
9 submitted only to the court ex parte and in  
10 camera:

11 “(I) Classified information.

12 “(II) Sensitive security informa-  
13 tion, as defined by section 1520.5 of  
14 title 49, Code of Federal Regulations.

15 “(III) Privileged law enforcement  
16 information.

17 “(IV) Information obtained or  
18 derived from any activity authorized  
19 under the Foreign Intelligence Sur-  
20 veillance Act of 1978 (50 U.S.C. 1801  
21 et seq.), except that, with respect to  
22 such information, subsections (c), (e),  
23 (f), (g), and (h) of section 106 (50  
24 U.S.C. 1806), subsections (d), (f), (g),  
25 (h), and (i) of section 305 (50 U.S.C.

1 1825), subsections (c), (e), (f), (g),  
2 and (h) of section 405 (50 U.S.C.  
3 1845), and section 706 (50 U.S.C.  
4 1881e) of that Act shall not apply.

5 “(V) Information subject to privi-  
6 lege or protections under any other  
7 provision of law.

8 “(iv) UNDER SEAL.—Any information  
9 that is part of the administrative record  
10 filed ex parte and in camera under clause  
11 (iii), or cited by the court in any decision,  
12 shall be treated by the court consistent  
13 with the provisions of this subparagraph  
14 and shall remain under seal and preserved  
15 in the records of the court to be made  
16 available consistent with the above provi-  
17 sions in the event of further proceedings.  
18 In no event shall such information be re-  
19 leased to the petitioner or as part of the  
20 public record.

21 “(v) RETURN.—After the expiration  
22 of the time to seek further review, or the  
23 conclusion of further proceedings, the  
24 court shall return the administrative

1 record, including any and all copies, to the  
2 United States.

3 “(C) EXCLUSIVE REMEDY.—A determina-  
4 tion by the court under this subsection shall be  
5 the exclusive judicial remedy for any claim de-  
6 scribed in this section against the United  
7 States, any United States department or agen-  
8 cy, or any component or official of any such de-  
9 partment or agency.

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

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

18 “(1) has the meaning given that term in section  
19 1(a) of the Classified Information Procedures Act  
20 (18 U.S.C. App.); and

21 “(2) includes—

22 “(A) any information or material that has  
23 been determined by the United States Govern-  
24 ment pursuant to an Executive order, statute,  
25 or regulation to require protection against un-



1 authorized disclosure for reasons of national se-  
 2 curity; and

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

6 **“§ 1328. Termination**

7 “This subchapter shall terminate on the date that is  
 8 5 years after the date of the enactment of the Federal  
 9 Acquisition Supply Chain Security Act of 2018.”.

10 (b) CLERICAL AMENDMENT.—The table of sections  
 11 at the beginning of chapter 13 of such title is amended  
 12 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.”.

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

18 (d) IMPLEMENTATION.—

19 (1) INTERIM FINAL RULE.—Not later than one  
 20 year after the date of the enactment of this Act, the

1 Federal Acquisition Security Council shall prescribe  
2 an interim final rule to implement subchapter III of  
3 chapter 13 of title 41, United States Code, as added  
4 by subsection (a).

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

12 (3) FAILURE TO ACT.—

13 (A) IN GENERAL.—If the Council does not  
14 issue a final rule in accordance with paragraph  
15 (2) on or before the last day of the one-year pe-  
16 riod referred to in that paragraph, the Council  
17 shall submit to the appropriate congressional  
18 committees and leadership, not later than 10  
19 days after such last day and every 90 days  
20 thereafter until the final rule is issued, a report  
21 explaining why the final rule was not timely  
22 issued and providing an estimate of the earliest  
23 date on which the final rule will be issued.

24 (B) APPROPRIATE CONGRESSIONAL COM-  
25 MITTEES AND LEADERSHIP DEFINED.—In this

1 paragraph, the term “appropriate congressional  
 2 committees and leadership” has the meaning  
 3 given that term in section 1321 of title 41,  
 4 United States Code, as added by subsection (a).

5 **SEC. 203. AUTHORITIES OF EXECUTIVE AGENCIES RELAT-**  
 6 **ING TO MITIGATING SUPPLY CHAIN RISKS IN**  
 7 **THE PROCUREMENT OF COVERED ARTICLES.**

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

11 **“§ 4713. Authorities relating to mitigating supply**  
 12 **chain risks in the procurement of cov-**  
 13 **ered articles**

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

17 “(b) DETERMINATION AND NOTIFICATION.—Except  
 18 as authorized by subsection (c) to address an urgent na-  
 19 tional security interest, the head of an executive agency  
 20 may exercise the authority provided in subsection (a) only  
 21 after—

22 “(1) obtaining a joint recommendation, in un-  
 23 classified or classified form, from the chief acquisi-  
 24 tion officer and the chief information officer of the  
 25 agency, or officials performing similar functions in

1 the case of executive agencies that do not have such  
2 officials, which includes a review of any risk assess-  
3 ment made available by the executive agency identi-  
4 fied under section 1323(a)(3) of this title, that there  
5 is a significant supply chain risk in a covered pro-  
6 curement;

7 “(2) providing notice of the joint recommenda-  
8 tion described in paragraph (1) to any source named  
9 in the joint recommendation advising—

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

12 “(B) to the extent consistent with the na-  
13 tional security and law enforcement interests, of  
14 information that forms the basis for the rec-  
15 ommendation;

16 “(C) that, within 30 days after receipt of  
17 the notice, the source may submit information  
18 and argument in opposition to the recommenda-  
19 tion; and

20 “(D) of the procedures governing the con-  
21 sideration of the submission and the possible  
22 exercise of the authority provided in subsection  
23 (a);

24 “(3) making a determination in writing, in un-  
25 classified or classified form, after considering any in-

1 formation submitted by a source under paragraph  
2 (2) and in consultation with the chief information  
3 security officer of the agency, that—

4 “(A) use of the authority under subsection  
5 (a) is necessary to protect national security by  
6 reducing supply chain risk;

7 “(B) less intrusive measures are not rea-  
8 sonably available to reduce such supply chain  
9 risk; and

10 “(C) the use of such authorities will apply  
11 to a single covered procurement or a class of  
12 covered procurements, and otherwise specifies  
13 the scope of the determination; and

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

18 “(A) the joint recommendation described  
19 in paragraph (1);

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

23 “(C) a summary of the basis for the deter-  
24 mination, including a discussion of less intru-  
25 sive measures that were considered and why

1           such measures were not reasonably available to  
2           reduce supply chain risk.

3           “(c) PROCEDURES TO ADDRESS URGENT NATIONAL  
4 SECURITY INTERESTS.—In any case in which the head of  
5 an executive agency determines that an urgent national  
6 security interest requires the immediate exercise of the au-  
7 thority provided in subsection (a), the head of the agen-  
8 cy—

9           “(1) may, to the extent necessary to address  
10          such national security interest, and subject to the  
11          conditions in paragraph (2)—

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

14               “(B) make the determination required by  
15               subsection (b)(3), regardless of whether the no-  
16               tice required by subsection (b)(2) has been pro-  
17               vided or whether the notified source has sub-  
18               mitted any information in response to such no-  
19               tice;

20               “(C) temporarily delay the notice required  
21               by subsection (b)(4); and

22               “(D) exercise the authority provided in  
23               subsection (a) in accordance with such deter-  
24               mination within 60 calendar days after the day  
25               the determination is made; and

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

5                   “(A) providing the notice required by sub-  
6                   section (b)(2);

7                   “(B) promptly considering any information  
8                   submitted by the source in response to such no-  
9                   tice, and making any appropriate modifications  
10                  to the determination based on such information;

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

16                  “(D) providing notice to the appropriate  
17                  congressional committees and leadership within  
18                  7 calendar days of the covered procurement ac-  
19                  tions taken under this section.

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

24           “(e) DELEGATION.—The head of an executive agency  
25           may not delegate the authority provided in subsection (a)

1 or the responsibility identified in subsection (f) to an offi-  
2 cial below the level one level below the Deputy Secretary  
3 or Principal Deputy Director.

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

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

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

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



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

5       “(k) DEFINITIONS.—In this section:

6               “(1) APPROPRIATE CONGRESSIONAL COMMIT-  
7 TEES AND LEADERSHIP.—The term ‘appropriate  
8 congressional committees and leadership’ means—

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

17                       “(B) the Committee on Oversight and Gov-  
18 ernment Reform, the Committee on the Judici-  
19 ary, the Committee on Appropriations, the  
20 Committee on Homeland Security, the Com-  
21 mittee on Armed Services, the Committee on  
22 Energy and Commerce, the Permanent Select  
23 Committee on Intelligence, and the Speaker and  
24 minority leader of the House of Representa-  
25 tives.

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

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

6           “(B) telecommunications equipment or  
7 telecommunications service, as those terms are  
8 defined in section 3 of the Communications Act  
9 of 1934 (47 U.S.C. 153);

10          “(C) the processing of information on a  
11 Federal or non-Federal information system,  
12 subject to the requirements of the Controlled  
13 Unclassified Information program; or

14          “(D) hardware, systems, devices, software,  
15 or services that include embedded or incidental  
16 information technology.

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

19          “(A) a source selection for a covered arti-  
20 cle involving either a performance specification,  
21 as provided in subsection (a)(3)(B) of section  
22 3306 of this title, or an evaluation factor, as  
23 provided in subsection (b)(1)(A) of such section,  
24 relating to a supply chain risk, or where supply  
25 chain risk considerations are included in the

1           agency’s determination of whether a source is a  
2           responsible source as defined in section 113 of  
3           this title;

4           “(B) the consideration of proposals for and  
5           issuance of a task or delivery order for a cov-  
6           ered article, as provided in section 4106(d)(3)  
7           of this title, where the task or delivery order  
8           contract includes a contract clause establishing  
9           a requirement relating to a supply chain risk;

10          “(C) any contract action involving a con-  
11          tract for a covered article where the contract in-  
12          cludes a clause establishing requirements relat-  
13          ing to a supply chain risk; or

14          “(D) any other procurement in a category  
15          of procurements determined appropriate by the  
16          Federal Acquisition Regulatory Council, with  
17          the advice of the Federal Acquisition Security  
18          Council.

19          “(4) COVERED PROCUREMENT ACTION.—The  
20          term ‘covered procurement action’ means any of the  
21          following actions, if the action takes place in the  
22          course of conducting a covered procurement:

23                 “(A) The exclusion of a source that fails to  
24                 meet qualification requirements established  
25                 under section 3311 of this title for the purpose

1 of reducing supply chain risk in the acquisition  
2 or use of covered articles.

3 “(B) The exclusion of a source that fails to  
4 achieve an acceptable rating with regard to an  
5 evaluation factor providing for the consideration  
6 of supply chain risk in the evaluation of pro-  
7 posals for the award of a contract or the  
8 issuance of a task or delivery order.

9 “(C) The determination that a source is  
10 not a responsible source as defined in section  
11 113 of this title based on considerations of sup-  
12 ply chain risk.

13 “(D) The decision to withhold consent for  
14 a contractor to subcontract with a particular  
15 source or to direct a contractor to exclude a  
16 particular source from consideration for a sub-  
17 contract under the contract.

18 “(5) INFORMATION AND COMMUNICATIONS  
19 TECHNOLOGY.—The term ‘information and commu-  
20 nications technology’ means—

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

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

1           “(C) telecommunications equipment and  
2           telecommunications services, as those terms are  
3           defined in section 3 of the Communications Act  
4           of 1934 (47 U.S.C. 153).

5           “(6) SUPPLY CHAIN RISK.—The term ‘supply  
6           chain risk’ means the risk that any person may sab-  
7           otage, maliciously introduce unwanted function, ex-  
8           tract data, or otherwise manipulate the design, in-  
9           tegrity, manufacturing, production, distribution, in-  
10          stallation, operation, maintenance, disposition, or re-  
11          tirement of covered articles so as to surveil, deny,  
12          disrupt, or otherwise manipulate the function, use,  
13          or operation of the covered articles or information  
14          stored or transmitted on the covered articles.

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

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

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

22          (c) EFFECTIVE DATE.—The amendments made by  
23          this section shall take effect on the date that is 90 days  
24          after the date of the enactment of this Act and shall apply

1 to contracts that are awarded before, on, or after that  
 2 date.

3 **SEC. 204. FEDERAL INFORMATION SECURITY MODERNIZA-**  
 4 **TION ACT.**

5 (a) IN GENERAL.—Title 44, United States Code, is  
 6 amended—

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

10 (2) in section 3554(a)(1)(B)—

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

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

16 (C) by adding at the end the following new  
 17 clause:

18 “(vi) responsibilities relating to as-  
 19 sessing and avoiding, mitigating, transfer-  
 20 ring, or accepting supply chain risks under  
 21 section 1326 of title 41, and complying  
 22 with exclusion and removal orders issued  
 23 under section 1323 of such title; and”.

24 (b) RULE OF CONSTRUCTION.—Nothing in this title  
 25 shall be construed to alter or impede any authority or re-

1 sponsibility under section 3553 of title 44, United States  
2 Code.

3 **SEC. 205. EFFECTIVE DATE.**

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

        Passed the House of Representatives December 19,  
2018.

Attest:

*Clerk.*

115<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

# H. R. 7327

---

## AN ACT

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.