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.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act'' or the ''SECURE Technology Act''.

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

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

SEC. 101. DEPARTMENT OF HOMELAND SECURITY DISCLOSURE OF SECURITY VULNERABILITIES.

(a) VULNERABILITY DISCLOSURE POLICY.—The Secretary of Homeland Security shall establish a policy appli-

cable to individuals, organizations, and companies that report security vulnerabilities on appropriate information systems of Department of Homeland Security. Such policy shall include each of the following:

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

(2) The conditions and criteria under which individuals, organizations, and companies may operate to discover and report security vulnerabilities.

(3) How individuals, organizations, and companies may disclose to the Department security vulnerabilities discovered on appropriate information systems of the Department.

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

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

(b) REMEDIATION PROCESS.—The Secretary of Homeland Security shall develop a process for the Department of Homeland Security to address the mitigation or remediation of the security vulnerabilities reported through the policy developed in subsection (a).

(c) CONSULTATION.—

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

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

(B) The Secretary of Defense and the Administrator of General Services regarding lessons that may be applied from existing vulnerability disclosure policies.

(C) Non-governmental security researchers.

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

(d) PUBLIC AVAILABILITY.—The Secretary of Homeland Security shall make the policy developed under subsection (a) publicly available.

(e) SUBMISSION TO CONGRESS.—

(1) DISCLOSURE POLICY AND REMEDIATION PROCESS.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to the appropriate congressional committees a copy of the policy required under subsection (a) and the remediation process required under subsection (b).

(2) REPORT AND BRIEFING.—

(A) REPORT.—Not later than one year after establishing the policy required under subsection (a), the Secretary of Homeland Security shall submit to the appropriate congressional committees a report on such policy and the remediation process required under subsection (b).

(B) ANNUAL BRIEFINGS.—One year after the date of the submission of the report under subparagraph (A), and annually thereafter for each of the next three years, the Secretary of Homeland Security shall provide to the appropriate congressional committees a briefing on the policy required under subsection (a) and the process required under subsection (b).

(C) MATTERS FOR INCLUSION.—The report required under subparagraph (A) and the

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

(i) The number of unique security vulnerabilities reported.

(ii) The number of previously unknown security vulnerabilities mitigated or remediated.

(iii) The number of unique individuals, organizations, and companies that reported security vulnerabilities.

(iv) The average length of time between the reporting of security vulnerabilities and mitigation or remediation of such vulnerabilities.

(f) DEFINITIONS.—In this section:

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

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

(3) The term ''appropriate information system'' means an information system that the Secretary of Homeland Security selects for inclusion under the vulnerability disclosure policy required by subsection (a).

(4) The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security, the Committee on Armed Services, the Committee on Energy and Commerce, and the Permanent Select Committee on Intelligence of the House of Representatives; and

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

SEC. 102. DEPARTMENT OF HOMELAND SECURITY BUG BOUNTY PILOT PROGRAM.

(a) DEFINITIONS.—In this section:

(1) The term ''appropriate congressional committees'' means—

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

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

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

(D) Permanent Select Committee on Intelligence of the House of Representatives.

(2) The term ''bug bounty program'' means a program under which—

(A) individuals, organizations, and companies are temporarily authorized to identify and report vulnerabilities of appropriate information systems of the Department; and

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

(3) The term ''Department'' means the Department of Homeland Security.

(4) The term ''eligible individual, organization, or company'' means an individual, organization, or company that meets such criteria as the Secretary determines in order to receive compensation in compliance with Federal laws.

(5) The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

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

(7) The term ''Secretary'' means the Secretary of Homeland Security.

(b) BUG BOUNTY PILOT PROGRAM.—

(1) ESTABLISHMENT.—Not later than 180 days after the date of enactment of this Act, the Secretary shall establish, within the Office of the Chief Information Officer, a bug bounty pilot program to minimize vulnerabilities of appropriate information systems of the Department.

(2) RESPONSIBILITIES OF SECRETARY.—In establishing and conducting the pilot program, the Secretary shall—

(A) designate appropriate information systems to be included in the pilot program;

(B) provide compensation to eligible individuals, organizations, and companies for reports of previously unidentified security vulnerabilities within the information systems designated under subparagraph (A);

(C) establish criteria for individuals, organizations, and companies to be considered eligible for compensation under the pilot program in compliance with Federal laws;

(D) consult with the Attorney General on how to ensure that approved individuals, organizations, or companies that comply with the requirements of the pilot program are protected from prosecution under section 1030 of title 18, United States Code, and similar provisions of law, and civil lawsuits for specific activities authorized under the pilot program;

(E) consult with the Secretary of Defense and the heads of other departments and agencies that have implemented programs to provide compensation for reports of previously undisclosed vulnerabilities in information systems, regarding lessons that may be applied from such programs; and

(F) develop an expeditious process by which an individual, organization, or company can register with the Department, submit to a background check as determined by the Department, and receive a determination as to eligibility; and

(G) engage qualified interested persons, including non-government sector representatives, about the structure of the pilot program as constructive and to the extent practicable.

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

(c) REPORT TO CONGRESS.—Not later than 180 days after the date on which the pilot program is completed, the Secretary shall submit to the appropriate congressional committees a report on the pilot program, which shall include—

(1) the number of individuals, organizations, or companies that participated in the pilot program, broken down by the number of individuals, organizations, or companies that—

(A) registered;

(B) were determined eligible;

(C) submitted security vulnerabilities; and

(D) received compensation;

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

(3) the number of previously unidentified security vulnerabilities remediated as a result of the pilot program;

(4) the current number of outstanding previously unidentified security vulnerabilities and Department remediation plans;

(5) the average length of time between the reporting of security vulnerabilities and remediation of the vulnerabilities;

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

(7) the lessons learned from the pilot program.

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

SEC. 103. CONGRESSIONAL SUBMITTAL OF REPORTS RELATING TO CERTAIN SPECIAL ACCESS PROGRAMS AND SIMILAR PROGRAMS.

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

(1) by striking ''Congress'' each place it appears and inserting ''the congressional oversight committees'';

(2) in subsection (f)(1), by striking ''appropriate oversight committees'' and inserting ''congressional oversight committees''; and

(3) in subsection (g)—

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

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

''(1) CONGRESSIONAL OVERSIGHT COMMITTEES.—The term 'congressional oversight committees' means—

''(A) congressional leadership and authorizing and appropriations congressional committees with jurisdiction or shared jurisdiction over a department or agency;

''(B) the Committee on Homeland Security and Governmental Affairs of the Senate; and

''(C) the Committee on Oversight and Government Reform of the House of Representatives.''.

TITLE II—FEDERAL ACQUISITION SUPPLY CHAIN SECURITY

SEC. 201. SHORT TITLE.

This title may be cited as the ''Federal Acquisition Supply Chain Security Act of 2018''.

SEC. 202. FEDERAL ACQUISITION SUPPLY CHAIN SECURITY.

(a) IN GENERAL.—Chapter 13 of title 41, United States Code, is amended by adding at the end the following new subchapter:

''SUBCHAPTER III—FEDERAL ACQUISITION SUPPLY CHAIN SECURITY

''§ 1321. Definitions

''In this subchapter:

''(1) APPROPRIATE CONGRESSIONAL COMMITTEES AND LEADERSHIP.—The term 'appropriate congressional committees and leadership' means—

''(A) the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Committee on Appropriations, the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, the Select Committee on Intelligence, and the majority and minority leader of the Senate; and

''(B) the Committee on Oversight and Government Reform, the Committee on the Judiciary, the Committee on Appropriations, the Committee on Homeland Security, the Committee on Armed Services, the Committee on Energy and Commerce, the Permanent Select Committee on Intelligence, and the Speaker and minority leader of the House of Representatives.

''(2) COUNCIL.—The term 'Council' means the Federal Acquisition Security Council established under section 1322(a) of this title.

''(3) COVERED ARTICLE.—The term 'covered article' has the meaning given that term in section 4713 of this title.

''(4) COVERED PROCUREMENT ACTION.—The term 'covered procurement action' has the meaning given that term in section 4713 of this title.

''(5) INFORMATION AND COMMUNICATIONS TECHNOLOGY.—The term 'information and communications technology' has the meaning given that term in section 4713 of this title.

''(6) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given that

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

''(7) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given that term in section 3552 of title 44.

''(8) SUPPLY CHAIN RISK.—The term 'supply chain risk' has the meaning given that term in section 4713 of this title.

''§ 1322. Federal Acquisition Security Council establishment and membership

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

''(b) MEMBERSHIP.—

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

''(A) The Office of Management and Budget.

''(B) The General Services Administration.

''(C) The Department of Homeland Security, including the Cybersecurity and Infrastructure Security Agency.

''(D) The Office of the Director of National Intelligence, including the National Counterintelligence and Security Center.

''(E) The Department of Justice, including the Federal Bureau of Investigation.

''(F) The Department of Defense, including the National Security Agency.

''(G) The Department of Commerce, including the National Institute of Standards and Technology.

''(H) Such other executive agencies as determined by the Chairperson of the Council.

''(2) LEAD REPRESENTATIVES.—

''(A) DESIGNATION.—

''(i) IN GENERAL.—Not later than 45 days after the date of the enactment of the Federal Acquisition Supply Chain Security Act of 2018, the head of each agency represented on the Council shall designate a representative of that agency as the lead representative of the agency on the Council.

''(ii) REQUIREMENTS.—The representative of an agency designated under clause (i) shall have expertise in supply chain risk management, acquisitions, or information and communications technology.

''(B) FUNCTIONS.—The lead representative of an agency designated under subparagraph (A) shall ensure that appropriate personnel, including leadership and subject matter experts of the agency, are aware of the business of the Council.

''(c) CHAIRPERSON.—

''(1) DESIGNATION.—Not later than 45 days after the date of the enactment of the Federal Acquisition Supply Chain Security Act of 2018, the Director of the Office of Management and Budget shall designate a senior-level official from the Office of Management and Budget to serve as the Chairperson of the Council.

''(2) FUNCTIONS.—The Chairperson shall perform functions that include—

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

''(B) designating executive agencies to be represented on the Council under subsection (b)(1)(H);

''(C) in consultation with the lead representative of each agency represented on the Council, developing a charter for the Council; and

''(D) not later than 7 days after completion of the charter, submitting the charter to the appropriate congressional committees and leadership.

''(d) MEETINGS.—The Council shall meet not later than 60 days after the date of the enactment of the Federal Acquisition Supply Chain Security Act of 2018 and not less frequently than quarterly thereafter.

''§ 1323. Functions and authorities

''(a) IN GENERAL.—The Council shall perform functions that include the following:

''(1) Identifying and recommending development by the National Institute of Standards and Technology of supply chain risk management standards, guidelines, and practices for executive agencies to use when assessing and developing mitigation strategies to address supply chain risks, particularly in the acquisition and use of covered articles under section 1326(a) of this title.

''(2) Identifying or developing criteria for sharing information with executive agencies, other Federal entities, and non-Federal entities with respect to supply chain risk, including information related to 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-

utive agencies taken under section 4713 of this title; and

''(D) inform the Council of orders issued under this section.

''(4) Identifying, as appropriate, executive agencies to provide—

''(A) shared services, such as support for making risk assessments, validation of products that may be suitable for acquisition, and mitigation activities; and

''(B) common contract solutions to support supply chain risk management activities, such as subscription services or machine-learning-enhanced analysis applications to support informed decision making.

''(5) Identifying and issuing guidance on additional steps that may be necessary to address supply chain risks arising in the course of executive agencies providing shared services, common contract solutions, acquisitions vehicles, or assisted acquisitions.

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

chain risks posed by the acquisition of covered articles.

''(7) Carrying out such other actions, as determined by the Council, that are necessary to reduce the supply chain risks posed by acquisitions and use of covered articles.

''(b) PROGRAM OFFICE AND COMMITTEES.—The Council may establish a program office and any committees, working groups, or other constituent bodies the Council deems appropriate, in its sole and unreviewable discretion, to carry out its functions.

''(c) AUTHORITY FOR EXCLUSION OR REMOVAL ORDERS.—

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

''(A) recommending orders applicable to executive agencies requiring the exclusion of sources or covered articles from executive agency procurement actions (in this section referred to as 'exclusion orders');

''(B) recommending orders applicable to executive agencies requiring the removal of covered articles from executive agency information

systems (in this section referred to as 'removal orders');

"(C) requesting and approving exceptions to an issued exclusion or removal order when warranted by circumstances, including alternative mitigation actions or other findings relating to the national interest, including national security reviews, national security investigations, or national security agreements; and

"(D) ensuring that recommended orders do not conflict with standards and guidelines issued under section 11331 of title 40 and that the Council consults with the Director of the National Institute of Standards and Technology regarding any recommended orders that would implement standards and guidelines developed by the National Institute of Standards and Technology.

"(2) RECOMMENDATIONS.—The Council shall use the criteria established under paragraph (1), information made available under subsection (a)(3), and any other information the Council determines appropriate to issue recommendations, for application to executive agencies or any subset thereof, regarding the exclusion of sources or covered articles

from any executive agency procurement action, including source selection and consent for a contractor to subcontract, or the removal of covered articles from executive agency information systems. Such recommendations shall include—

"(A) information necessary to positively identify the sources or covered articles recommended for exclusion or removal;

"(B) information regarding the scope and applicability of the recommended exclusion or removal order;

"(C) a summary of any risk assessment reviewed or conducted in support of the recommended exclusion or removal order;

"(D) a summary of the basis for the recommendation, including a discussion of less intrusive measures that were considered and why such measures were not reasonably available to reduce supply chain risk;

"(E) a description of the actions necessary to implement the recommended exclusion or removal order; and

"(F) where practicable, in the Council's sole and unreviewable discretion, a description of mitigation steps that could be taken by the

source that may result in the Council rescinding a recommendation.

''(3) NOTICE OF RECOMMENDATION AND REVIEW.—A notice of the Council's recommendation under paragraph (2) shall be issued to any source named in the recommendation advising—

''(A) that a recommendation has been made;

''(B) of the criteria the Council relied upon under paragraph (1) and, to the extent consistent with national security and law enforcement interests, of information that forms the basis for the recommendation;

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

''(D) of the procedures governing the review and possible issuance of an exclusion or removal order pursuant to paragraph (5); and

''(E) where practicable, in the Council's sole and unreviewable discretion, a description of mitigation steps that could be taken by the source that may result in the Council rescinding the recommendation.

''(4) CONFIDENTIALITY.—Any notice issued to a source under paragraph (3) shall be kept confidential until—

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

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

''(5) EXCLUSION AND REMOVAL ORDERS.—

''(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:

''(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).

''(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.

"(iii) The Director of National Intelligence, for exclusion and removal orders applicable to the intelligence community and sensitive compartmented information systems, to the extent not covered by clause (ii).

"(B) DELEGATION.—The officials identified in subparagraph (A) may not delegate any authority under this subparagraph to an official below the level one level below the Deputy Secretary or Principal Deputy Director, except that the Secretary of Defense may delegate authority for removal orders to the Commander of the United States Cyber Command, who may not redelegate such authority to an official below the level one level below the Deputy Commander.

"(C) FACILITATION OF EXCLUSION ORDERS.—If officials identified under this paragraph from the Department of Homeland Security, the Department of Defense, and the Office of the Director of National Intelligence issue orders collectively resulting in a governmentwide exclusion, the Administrator for General Services and officials at other executive agencies re-

sponsible for management of the Federal Supply Schedules, governmentwide acquisition contracts and multi-agency contracts shall help facilitate implementation of such orders by removing the covered articles or sources identified in the orders from such contracts.

''(D) REVIEW OF EXCLUSION AND REMOVAL ORDERS.—The officials identified under this paragraph shall review all exclusion and removal orders issued under subparagraph (A) not less frequently than annually pursuant to procedures established by the Council.

''(E) RESCISSION.—Orders issued pursuant to subparagraph (A) may be rescinded by an authorized official from the relevant issuing agency.

''(6) NOTIFICATIONS.—Upon issuance of an exclusion or removal order pursuant to paragraph (5)(A), the official identified under that paragraph who issued the order shall—

''(A) notify any source named in the order of—

''(i) the exclusion or removal order; and

"(ii) to the extent consistent with national security and law enforcement interests, information that forms the basis for the order;

"(B) provide classified or unclassified notice of the exclusion or removal order to the appropriate congressional committees and leadership; and

"(C) provide the exclusion or removal order to the agency identified in subsection (a)(3).

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

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

"(e) RELATIONSHIP TO OTHER COUNCILS.—The Council shall consult and coordinate, as appropriate, with other relevant councils and interagency committees, including the Chief Information Officers Council, the Chief Acquisition Officers Council, the Federal Acquisition Regulatory Council, and the Committee on Foreign Invest-

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

''(f) RULES OF CONSTRUCTION.—Nothing in this section shall be construed—

''(1) to limit the authority of the Office of Federal Procurement Policy to carry out the responsibilities of that Office under any other provision of law; or

''(2) to authorize the issuance of an exclusion or removal order based solely on the fact of foreign ownership of a potential procurement source that is otherwise qualified to enter into procurement contracts with the Federal Government.

''§ 1324. Strategic plan

''(a) IN GENERAL.—Not later than 180 days after the date of the enactment of the Federal Acquisition Supply Chain Security Act of 2018, the Council shall develop a strategic plan for addressing supply chain risks posed by the acquisition of covered articles and for managing such risks that includes—

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

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

''(2) an identification of existing authorities for addressing such risks;

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

''(4) recommendations for any legislative, regulatory, or other policy changes to improve efforts to address such risks;

''(5) recommendations for any legislative, regulatory, or other policy changes to incentivize the adoption of best practices for supply chain risk management by the private sector;

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

''(7) a plan for engaging with executive agencies, the private sector, and other nongovernmental stakeholders to address such risks;

''(8) a plan for identification, assessment, mitigation, and vetting of supply chain risks from existing and prospective information and communications technology made available by executive agencies to other executive agencies through common contract

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

''(9) plans to strengthen the capacity of all executive agencies to conduct assessments of—

''(A) the supply chain risk posed by the acquisition of covered articles; and

''(B) compliance with the requirements of this subchapter.

''(b) SUBMISSION TO CONGRESS.—Not later than 7 calendar days after completion of the strategic plan required by subsection (a), the Chairperson of the Council shall submit the plan to the appropriate congressional committees and leadership.

''§ 1325. Annual report

''Not later than December 31 of each year, the Chairperson of the Council shall submit to the appropriate congressional committees and leadership a report on the activities of the Council during the preceding 12-month period.

''§ 1326. Requirements for executive agencies

''(a) IN GENERAL.—The head of each executive agency shall be responsible for—

''(1) assessing the supply chain risk posed by the acquisition and use of covered articles and avoiding, mitigating, accepting, or transferring that risk,

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

''(2) prioritizing supply chain risk assessments conducted under paragraph (1) based on the criticality of the mission, system, component, service, or asset.

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

''(1) developing an overall supply chain risk management strategy and implementation plan and policies and processes to guide and govern supply chain risk management activities;

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

''(3) limiting, avoiding, mitigating, accepting, or transferring any identified risk;

''(4) sharing relevant information with other executive agencies as determined appropriate by the Council in a manner consistent with section 1323(a) of this title;

''(5) reporting on progress and effectiveness of the agency's supply chain risk management con-

sistent with guidance issued by the Office of Management and Budget and the Council; and

''(6) ensuring that all relevant information, including classified information, with respect to acquisitions of covered articles that may pose a supply chain risk, consistent with section 1323(a) of this title, is incorporated into existing processes of the agency for conducting assessments described in subsection (a) and ongoing management of acquisition programs, including any identification, investigation, mitigation, or remediation needs.

''(c) INTERAGENCY ACQUISITIONS.—

''(1) IN GENERAL.—Except as provided in paragraph (2), in the case of an interagency acquisition, subsection (a) shall be carried out by the head of the executive agency whose funds are being used to procure the covered article.

''(2) ASSISTED ACQUISITIONS.—In an assisted acquisition, the parties to the acquisition shall determine, as part of the interagency agreement governing the acquisition, which agency is responsible for carrying out subsection (a).

''(3) DEFINITIONS.—In this subsection, the terms 'assisted acquisition' and 'interagency acquisition' have the meanings given those terms in section

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

''(d) ASSISTANCE.—The Secretary of Homeland Security may—

''(1) assist executive agencies in conducting risk assessments described in subsection (a) and implementing mitigation requirements for information and communications technology; and

''(2) provide such additional guidance or tools as are necessary to support actions taken by executive agencies.

''§ 1327. Judicial review procedures

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

''(b) PETITIONS.—

''(1) IN GENERAL.—Not later than 60 days after a party is notified of an exclusion or removal order under section 1323(c)(6) of this title or a covered procurement action under section 4713 of this

title, the party may file a petition for judicial review in the United States Court of Appeals for the District of Columbia Circuit claiming that the issuance of the exclusion or removal order or covered procurement action is unlawful.

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

''(A) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law;

''(B) contrary to constitutional right, power, privilege, or immunity;

''(C) in excess of statutory jurisdiction, authority, or limitation, or short of statutory right;

''(D) lacking substantial support in the administrative record taken as a whole or in classified information submitted to the court under paragraph (3); or

''(E) not in accord with procedures required by law.

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

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

''(4) ADMINISTRATIVE RECORD AND PROCEDURES.—

''(A) IN GENERAL.—The procedures described in this paragraph shall apply to the review of a petition under this section.

''(B) ADMINISTRATIVE RECORD.—

''(i) FILING OF RECORD.—The United States shall file with the court an administrative record, which shall consist of the information that the appropriate official relied upon in issuing an exclusion or removal order under section 1323(c)(5) or a covered procurement action under section 4713 of this title.

''(ii) UNCLASSIFIED, NONPRIVILEGED INFORMATION.—All unclassified information contained in the administrative record that is not otherwise privileged or subject

to statutory protections shall be provided to the petitioner with appropriate protections for any privileged or confidential trade secrets and commercial or financial information.

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

''(I) Classified information.

''(II) Sensitive security information, as defined by section 1520.5 of title 49, Code of Federal Regulations.

''(III) Privileged law enforcement information.

''(IV) Information obtained or derived from any activity authorized under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), except that, with respect to such information, subsections (c), (e), (f), (g), and (h) of section 106 (50 U.S.C. 1806), subsections (d), (f), (g), (h), and (i) of section 305 (50 U.S.C.

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

''(V) Information subject to privilege or protections under any other provision of law.

''(iv) UNDER SEAL.—Any information that is part of the administrative record filed ex parte and in camera under clause (iii), or cited by the court in any decision, shall be treated by the court consistent with the provisions of this subparagraph and shall remain under seal and preserved in the records of the court to be made available consistent with the above provisions in the event of further proceedings. In no event shall such information be released to the petitioner or as part of the public record.

''(v) RETURN.—After the expiration of the time to seek further review, or the conclusion of further proceedings, the court shall return the administrative

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

''(C) EXCLUSIVE REMEDY.—A determination by the court under this subsection shall be the exclusive judicial remedy for any claim described in this section against the United States, any United States department or agency, or any component or official of any such department or agency.

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

''(c) DEFINITION.—In this section, the term 'classified information'—

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

''(2) includes—

''(A) any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation to require protection against un-

authorized disclosure for reasons of national security; and

''(B) any restricted data, as defined in section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014).

''§ 1328. Termination

''This subchapter shall terminate on the date that is 5 years after the date of the enactment of the Federal Acquisition Supply Chain Security Act of 2018.''.

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

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

(d) IMPLEMENTATION.—

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

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

(2) FINAL RULE.—Not later than one year after prescribing the interim final rule under paragraph (1) and considering public comments with respect to such interim final rule, the Council shall prescribe a final rule to implement subchapter III of chapter 13 of title 41, United States Code, as added by subsection (a).

(3) FAILURE TO ACT.—

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

(B) APPROPRIATE CONGRESSIONAL COMMITTEES AND LEADERSHIP DEFINED.—In this

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

SEC. 203. AUTHORITIES OF EXECUTIVE AGENCIES RELATING TO MITIGATING SUPPLY CHAIN RISKS IN THE PROCUREMENT OF COVERED ARTICLES.

(a) IN GENERAL.—Chapter 47 of title 41, United States Code, is amended by adding at the end the following new section:

''§ 4713. Authorities relating to mitigating supply chain risks in the procurement of covered articles

''(a) AUTHORITY.—Subject to subsection (b), the head of an executive agency may carry out a covered procurement action.

''(b) DETERMINATION AND NOTIFICATION.—Except as authorized by subsection (c) to address an urgent national security interest, the head of an executive agency may exercise the authority provided in subsection (a) only after—

''(1) obtaining a joint recommendation, in unclassified or classified form, from the chief acquisition officer and the chief information officer of the agency, or officials performing similar functions in

the case of executive agencies that do not have such officials, which includes a review of any risk assessment made available by the executive agency identified under section 1323(a)(3) of this title, that there is a significant supply chain risk in a covered procurement;

''(2) providing notice of the joint recommendation described in paragraph (1) to any source named in the joint recommendation advising—

''(A) that a recommendation is being considered or has been obtained;

''(B) to the extent consistent with the national security and law enforcement interests, of information that forms the basis for the recommendation;

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

''(D) of the procedures governing the consideration of the submission and the possible exercise of the authority provided in subsection (a);

''(3) making a determination in writing, in unclassified or classified form, after considering any in-

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

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

"(B) less intrusive measures are not reasonably available to reduce such supply chain risk; and

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

"(4) providing a classified or unclassified notice of the determination made under paragraph (3) to the appropriate congressional committees and leadership that includes—

"(A) the joint recommendation described in paragraph (1);

"(B) a summary of any risk assessment reviewed in support of the joint recommendation required by paragraph (1); and

"(C) a summary of the basis for the determination, including a discussion of less intrusive measures that were considered and why

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

''(c) PROCEDURES TO ADDRESS URGENT NATIONAL SECURITY INTERESTS.—In any case in which the head of an executive agency determines that an urgent national security interest requires the immediate exercise of the authority provided in subsection (a), the head of the agency—

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

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

''(B) make the determination required by subsection (b)(3), regardless of whether the notice required by subsection (b)(2) has been provided or whether the notified source has submitted any information in response to such notice;

''(C) temporarily delay the notice required by subsection (b)(4); and

''(D) exercise the authority provided in subsection (a) in accordance with such determination within 60 calendar days after the day the determination is made; and

''(2) shall take actions necessary to comply with all requirements of subsection (b) as soon as practicable after addressing the urgent national security interest, including—

''(A) providing the notice required by subsection (b)(2);

''(B) promptly considering any information submitted by the source in response to such notice, and making any appropriate modifications to the determination based on such information;

''(C) providing the notice required by subsection (b)(4), including a description of the urgent national security interest, and any modifications to the determination made in accordance with subparagraph (B); and

''(D) providing notice to the appropriate congressional committees and leadership within 7 calendar days of the covered procurement actions taken under this section.

''(d) CONFIDENTIALITY.—The notice required by subsection (b)(2) shall be kept confidential until a determination with respect to a covered procurement action has been made pursuant to subsection (b)(3).

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

or the responsibility identified in subsection (f) to an official below the level one level below the Deputy Secretary or Principal Deputy Director.

''(f) ANNUAL REVIEW OF DETERMINATIONS.—The head of an executive agency shall conduct an annual review of all determinations made by such head under subsection (b) and promptly amend any covered procurement action as appropriate.

''(g) REGULATIONS.—The Federal Acquisition Regulatory Council shall prescribe such regulations as may be necessary to carry out this section.

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

''(i) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to authorize the head of an executive agency to carry out a covered procurement action based solely on the fact of foreign ownership of a potential procurement source that is otherwise qualified to enter into procurement contracts with the Federal Government.

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

''(k) DEFINITIONS.—In this section:

''(1) APPROPRIATE CONGRESSIONAL COMMITTEES AND LEADERSHIP.—The term 'appropriate congressional committees and leadership' means—

''(A) the Committee on Homeland Security and Governmental Affairs, the Committee on the Judiciary, the Committee on Appropriations, the Committee on Armed Services, the Committee on Commerce, Science, and Transportation, the Select Committee on Intelligence, and the majority and minority leader of the Senate; and

''(B) the Committee on Oversight and Government Reform, the Committee on the Judiciary, the Committee on Appropriations, the Committee on Homeland Security, the Committee on Armed Services, the Committee on Energy and Commerce, the Permanent Select Committee on Intelligence, and the Speaker and minority leader of the House of Representatives.

''(2) COVERED ARTICLE.—The term 'covered article' means—

''(A) information technology, as defined in section 11101 of title 40, including cloud computing services of all types;

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

''(C) the processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program; or

''(D) hardware, systems, devices, software, or services that include embedded or incidental information technology.

''(3) COVERED PROCUREMENT.—The term 'covered procurement' means—

''(A) a source selection for a covered article involving either a performance specification, as provided in subsection (a)(3)(B) of section 3306 of this title, or an evaluation factor, as provided in subsection (b)(1)(A) of such section, relating to a supply chain risk, or where supply chain risk considerations are included in the

agency's determination of whether a source is a responsible source as defined in section 113 of this title;

"(B) the consideration of proposals for and issuance of a task or delivery order for a covered article, as provided in section 4106(d)(3) of this title, where the task or delivery order contract includes a contract clause establishing a requirement relating to a supply chain risk;

"(C) any contract action involving a contract for a covered article where the contract includes a clause establishing requirements relating to a supply chain risk; or

"(D) any other procurement in a category of procurements determined appropriate by the Federal Acquisition Regulatory Council, with the advice of the Federal Acquisition Security Council.

"(4) COVERED PROCUREMENT ACTION.—The term 'covered procurement action' means any of the following actions, if the action takes place in the course of conducting a covered procurement:

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

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

''(B) The exclusion of a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a task or delivery order.

''(C) The determination that a source is not a responsible source as defined in section 113 of this title based on considerations of supply chain risk.

''(D) The decision to withhold consent for a contractor to subcontract with a particular source or to direct a contractor to exclude a particular source from consideration for a subcontract under the contract.

''(5) INFORMATION AND COMMUNICATIONS TECHNOLOGY.—The term 'information and communications technology' means—

''(A) information technology, as defined in section 11101 of title 40;

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

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

''(6) SUPPLY CHAIN RISK.—The term 'supply chain risk' means the risk that any person may sabotage, maliciously introduce unwanted function, extract data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the covered articles or information stored or transmitted on the covered articles.

''(7) EXECUTIVE AGENCY.—Notwithstanding section 3101(c)(1), this section applies to the Department of Defense, the Coast Guard, and the National Aeronautics and Space Administration.''.

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

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

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

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

SEC. 204. FEDERAL INFORMATION SECURITY MODERNIZATION ACT.

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

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

(2) in section 3554(a)(1)(B)—

(A) by inserting '', subchapter III of chapter 13 of title 41,'' after ''complying with the requirements of this subchapter'';

(B) in clause (iv), by striking ''; and'' and inserting a semicolon; and

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

''(vi) responsibilities relating to assessing and avoiding, mitigating, transferring, or accepting supply chain risks under section 1326 of title 41, and complying with exclusion and removal orders issued under section 1323 of such title; and''.

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

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

SEC. 205. EFFECTIVE DATE.

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

Passed the House of Representatives December 19, 2018.

Attest:

Clerk.

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.