116TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
116–188

SECURING THE HOMELAND SECURITY SUPPLY CHAIN ACT OF 2019

AUGUST 27, 2019.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. THOMPSON of Mississippi, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 3320]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 3320) to amend the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security to implement certain requirements for information relating to supply chain risk, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Securing the Homeland Security Supply Chain Act of 2019".

SEC. 2. DEPARTMENT OF HOMELAND SECURITY REQUIREMENTS FOR INFORMATION RELATING TO SUPPLY CHAIN RISK.

(a) IN GENERAL.—Subtitle D of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 391 et seq.) is amended by adding at the end the following new section:

"SEC. 836. REQUIREMENTS FOR INFORMATION RELATING TO SUPPLY CHAIN RISK.

"(a) AUTHORITY.—Subject to subsection (b), the Secretary may—

"(1) carry out a covered procurement action;

"(2) limit, notwithstanding any other provision of law, in whole or in part, the disclosure of information, including classified information, relating to the basis for carrying out such an action; and

"(3) exclude, in whole or in part, a source carried out in the course of such an action applicable to a covered procurement of the Department.

"(b) DETERMINATION AND NOTIFICATION.—Except as authorized by subsection (c) to address an urgent national security interest, the Secretary 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 Department, including a review of any risk assessment made available by an appropriate person or entity, including the national risk management center at the Cybersecurity and Infrastructure Security Agency, that there is a significant supply chain risk in a covered procurement;

"(2) notifying any source named in the joint recommendation described in paragraph (1) advising—

"(A) that a recommendation has been obtained;

"(B) to the extent consistent with the national security and law enforcement interests, the basis for such recommendation;

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

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

"(3) notifying the relevant components of the Department that such risk assessment has demonstrated significant supply chain risk to a covered procurement;

"(4) making a determination in writing, in unclassified or classified form, that after considering any information submitted by a source under paragraph (2), and in consultation with the Chief Information Officer of the Department, that—

"(A) use of authority under subsection (a)(1) is necessary to protect national security by reducing supply chain risk;

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

"(C) a decision to limit disclosure of information under subsection (a)(2) is necessary to protect national security interest; and

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

"(5) providing to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a classified or unclassified notice of the determination made under paragraph (4) that includes—

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

"(B) a summary of any risk assessment reviewed in support of such joint recommendation; and

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

"(6) notifying the Director of the Office of Management and Budget, and the heads of other Federal agencies as appropriate, in a manner and to the extent consistent with the requirements of national security; and

"(7) taking steps to maintain the confidentiality of any notifications under this subsection.

"(c) PROCEDURES TO ADDRESS URGENT NATIONAL SECURITY INTERESTS.—In any case in which the Secretary determines that national security interests require the immediate exercise of the authorities under subsection (a), the Secretary—

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

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

"(B) make the determination required by subsection (b)(4), regardless of whether the notice required by subsection (b)(2) has been provided or whether the notified source at issue has submitted any information in response to such notice;

"(C) temporarily delay the notice required by subsections (b)(4) and (b)(5); and

"(D) exercise the authority provided in subsection (a) in accordance with such determination; 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 that is the subject of paragraph (1), including—

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

"(B) promptly considering any information submitted by the source at issue in response to such notice, and making any appropriate modifications to the determination required by subsection (b)(4) based on such information; and

"(C) providing the notice required by subsections (b)(5) and (b)(6), including a description of such urgent national security, and any modifications to such determination made in accordance with subparagraph (B).

"(d) ANNUAL REVIEW OF DETERMINATIONS.—The Secretary shall annually review all determinations made under subsection (b).

"(e) DELEGATION.—The Secretary may not delegate the authority provided in subsection (a) or the responsibility identified in subsection (d) to an official below the Deputy Secretary.

"(f) LIMITATION OF REVIEW.—Notwithstanding any other provision of law, no action taken by the Secretary under subsection (a) may be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

"(g) CONSULTATION.—In developing procedures and guidelines for the implementation of the authorities described in this section, the Secretary shall review the procedures and guidelines utilized by the Department of Defense to carry out similar authorities.

"(h) DEFINITIONS.—In this section:

"(1) COVERED ARTICLE.—The term 'covered article' means:

"(A) Information technology, including cloud computing services of all types.

"(B) Telecommunications equipment.

"(C) Telecommunications services.

"(D) The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program of the Department.

"(E) Hardware, systems, devices, software, or services that include embedded or incidental information technology.

"(2) 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 title 41, United States Code, or an evaluation factor, as provided in subsection (c)(1)(A) of such section, relating to supply chain risk, or with respect to which supply chain risk considerations are included in the Department's determination of whether a source is a responsible source as defined in section 113 of such 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 title 41, United States Code, with respect to which the task or delivery order contract includes a contract clause establishing a requirement relating to supply chain risk;

"(C) any contract action involving a contract for a covered article with respect to which such contract includes a clause establishing requirements relating to supply chain risk; or

"(D) any procurement made via Government Purchase Care for a covered article when supply chain risk has been identified as a concern.

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

"(A) The exclusion of a source that fails to meet qualification requirements established pursuant to section 3311 of title 41, United States Code,

for the purpose of reducing supply chain risk in the acquisition or use of a covered article.

"(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 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.

"(4) INFORMATION SYSTEM.—The term 'information system' has the meaning given such term in section 3502 of title 44, United States Code.

"(5) INFORMATION TECHNOLOGY.—The term 'information technology' has the meaning given such term in section 11101 of title 40, United States Code.

"(6) RESPONSIBLE SOURCE.—The term 'responsible source' has the meaning given such term in section 113 of title 41, United States Code.

"(7) SUPPLY CHAIN RISK.—The term 'supply chain risk' means the risk that a malicious actor may sabotage, maliciously introduce an unwanted function, extract or modify data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered article so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the information technology or information stored or transmitted on the covered articles.

"(8) TELECOMMUNICATIONS EQUIPMENT.—The term 'telecommunications equipment' has the meaning given such term in section 3(52) of the Communications Act of 1934 (47 U.S.C. 153(52)).

"(9) TELECOMMUNICATIONS SERVICE.—The term 'telecommunications service' has the meaning given such term in section 3(53) of the Communications Act of 1934 (47 U.S.C. 153(53)).

"(i) EFFECTIVE DATE.—The requirements of 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—

"(1) contracts awarded on or after such date; and

"(2) task and delivery orders issued on or after such date pursuant to contracts awarded before, on, or after such date.".

(b) RULEMAKING.—Section 553 of title 5, United States Code, and section 1707 of title 41, United States Code, shall not apply to the Secretary of Homeland Security when carrying out the authorities and responsibilities under section 836 of the Homeland Security Act of 2002, as added by subsection (a).

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 835 the following new item:

"Sec. 836. Requirements for information relating to supply chain risk.".

SEC. 3. REPORT ON THREATS POSED BY FOREIGN STATE-OWNED ENTITIES TO DHS INFORMATION TECHNOLOGY AND COMMUNICATIONS SYSTEMS.

Not later than 180 days after the date of the enactment of this Act, the Under Secretary for Management of the Department of Homeland Security, in coordination with the national risk management center of the Cybersecurity and Infrastructure Security Agency of the Department, shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on cybersecurity threats posed by terrorist actors and foreign state-owned entities to the information technology and communications systems of Department of Homeland Security, including information relating to the following:

(1) The use of foreign state-owned entities' information and communications technology by the Department of Homeland Security, listed by component.

(2) The threats, in consultation with the Department's Office of Intelligence and Analysis, of foreign state-owned entities' information and communications technology equipment that could impact the Department.

PURPOSE AND SUMMARY

The purpose of H.R. 3320, the "Securing the Homeland Security Supply Chain Act of 2019," is to provide the Secretary of Homeland Security with the authority to restrict certain procurements related to information technology and associated products if, following a risk assessment, it is determined the vendor poses a threat to the

Department of Homeland Security supply chain. If such a determination is made, the Secretary is permitted to limit the amount of information disclosed about the decision-making process.

BACKGROUND AND NEED FOR LEGISLATION

Federal agencies rely on vendors to provide them with products and services to carry out their missions and the Department of Homeland Security (DHS or Department) is no exception. This reliance could put DHS at risk if the products and services supplied are exploited to introduce vulnerabilities into the Department's supply chain. Recent reports about potential supply chain threats linked to foreign-based firms, especially ones in China and Russia, highlight the pervasive and growing threats to the federal supply chain.

Chinese companies, a number of whom are state-owned or have extensive ties to the Chinese state, are leaders in a number of advanced technology fields. For years, the Intelligence Community has warned that information and communication technology (ICT) produced by certain Chinese companies, most notably the two largest Chinese telecommunications equipment manufacturers, ZTE Corporation and Huawei, could be used to carry out cyber theft, spying, and espionage.[1] Some companies with ties to the Russian government also pose national security risks. The U.S. government has particularly highlighted concerns about Kaspersky labs.[2] According to DHS, Kaspersky anti-virus products could be exploited by malicious cyber actors to compromise information systems, and the Russian government could use Kaspersky to compromise federal information systems, directly implicating U.S. national security.[3] In September 2017, DHS issued a Binding Operational Directive (BOD) requiring Federal agencies to remove all Kaspersky products from their networks due to Russia-related supply chain concerns.[4]

In response to these supply chain concerns, H.R. 3320 would provide the Secretary of Homeland Security with the authority to restrict certain procurements related to information technology and associated products if, following a risk assessment, it is determined the vendor poses a threat to the DHS supply chain.

HEARINGS

For the purposes of section 103(i) of H. Res. 6 of the 116th Congress, the following hearing was used to develop or consider H.R. 3320:

On Thursday, July 12, 2018, the Subcommittee on Counterterrorism and Intelligence and the Subcommittee on Oversight and Management Efficiency of the Committee on Homeland Security held a hearing entitled "Access Denied: Keeping Adversaries Away from the Homeland Security Supply Chain". The Subcommittees

---

[1] U.S. House of Representatives Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,* 112th Cong. (Oct. 8, 2012), available at https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

[2] DHS Statement on the Issuance of Binding Operational Directive 17–01, U.S. Department of Homeland Security, (Sept. 13, 2017), available at https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01.

[3] Ibid.

[4] See 82 Fed. Reg. 42782.

received testimony from Ms. Soraya Correa, Chief Procurement Officer; Dr. John Zangardi, Chief Information Officer; Ms. Jeanette Manfra, Assistant Secretary in the Office of Cybersecurity and Communications, National Protection and Programs Directorate; Ms. Tina W. Gabbrielli, Acting Deputy Under Secretary for Intelligence Enterprise Operations; and Mr. Gregory Wilshusen, Director of Information Security Issues, Government Accountability Office.

COMMITTEE CONSIDERATION

The Committee met on July 17, 2019, with a quorum being present, to consider H.R. 3320 and ordered the measure to be reported to the House with a favorable recommendation, with amendment, by unanimous consent.

The following Amendments were offered and accepted by unanimous consent:

An amendment offered by Ms. Jackson Lee.

Page 3, line 2, insert "including the national risk management center at the Cybersecurity and Infrastructure Security Agency," after "tity". Add at the end the following:

SEC. 3. REPORT ON THREATS POSED BY FOREIGN STATE-OWNED ENTITIES TO DHS INFORMATION TECHNOLOGY AND COMMUNICATIONS SYSTEMS.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 3320.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

CONGRESSIONAL BUDGET OFFICE ESTIMATE, NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements of clause (3)(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 30, 2019.

Hon. BENNIE G. THOMPSON,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for Department of Homeland Security Legislation.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

Department of Homeland Security Legislation
As ordered reported by the House Committee on Homeland Security on July 17, 2019

By Fiscal Year, Millions of Dollars	2019	2019-2024	2019-2029
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	*	not estimated

Statutory pay-as-you-go procedures apply?	No	Mandate Effects	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2030?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = less than $500,000; the table above applies to each bill described below.

On July 17, 2019, the House Committee on Homeland Security ordered reported the following bills:

- H.R. 3320, the Securing the Homeland Security Supply Chain Act of 2019, which would authorize the Department of Homeland Security (DHS) to take certain actions to improve the security of information and telecommunications systems acquired by the department;
- H.R. 3413, DHS Acquisition Reform Act of 2019, which would specify which offices in DHS headquarters have responsibility for acquisition programs;
- H.R. 3526, the Counter Terrorist Network Act, which would authorize Customs and Border Protection to assign personnel to other agencies to support partnerships for sharing global information to enhance border security; and
- H.R. 3722, the Joint Task Force to Combat Opioid Trafficking Act of 2019, which would confirm the authority of DHS to establish a task force to disrupt drug trafficking.

DHS is currently carrying out activities similar to those required by the bills listed above, and any new activities required under the legislation would not require substantial action by the department.

Thus, CBO estimates that implementing each bill would not have a significant cost; any spending would be subject to the availability of appropriated funds.

The CBO staff contact for this estimate is Mark Grabowicz. The estimate was reviewed by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 3320 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

PERFORMANCE GOALS AND OBJECTIVES

The Committee states that pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 3320 would amend the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security to restrict certain procurements related to information technology and associated products if it is determined that the procurement poses a national security risk. The bill requires the Secretary to notify the appropriate Committees of the Senate and House of Representatives, as well as the Office of Management and Budget and the vendor of the risk determination. The bill also requires the Secretary to review existing procedures and guidelines used by the Department of Defense when developing the procedures and guidelines for the Department of Homeland Security. Lastly, the bill requires the Secretary to review any supply chain restrictions determined under the Act on an annual basis.

ADVISORY ON EARMARKS

In compliance with rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of the rule XXI.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section provides that this bill may be cited as the "Securing the Homeland Security Supply Chain Act of 2019".

Sec. 2. Department of Homeland Security requirements for information relating to supply chain risk

This section establishes a new Section 836 in the Homeland Security Act as follows:

Subsection (a) authorizes the Secretary of Homeland Security to take the following actions related to the procurement of a covered article, which includes information technology, telecommunications equipment, telecommunication services, and associated hardware, software, and services: exclude a source

from the procurement process if the source fails to meet established supply chain risk standards or is determined not to be a responsible source; and direct a contractor to exclude a particular source for a subcontract; limit the information disclosed, including classified information, about the basis for carrying out a covered procurement action; and exclude a source, if identified to be a threat, from procurements or contracts across the Department.

Subsection (b) authorizes the DHS Secretary to take the action permitted in subsection (a) only after: obtaining a joint recommendation from the Department's Chief Acquisition Officer and Chief Information Officer that there is a significant supply chain risk in a covered procurement; providing notice of the recommendation to any source named in such recommendation and allowing that source 30 days to submit information in response; notifying the relevant Departmental components of the risk; documenting in writing the determination that the use of the authority is necessary; there are no less intrusive measures available to reduce the risk; that disclosing information about the risk and the procurement would pose a greater risk to national security; and whether the exclusion will apply to a single covered procurement or a class of covered procurements; providing notice of the determination to the Committee on Homeland Security of the House and the Committee on Homeland Security and Governmental Affairs of the Senate; notifying the Director of the Office of Management and Budget, and other appropriate Federal agencies; and taking steps necessary to maintain the confidentiality of any notifications made under this subsection.

Subsection (c) allows the Secretary to delay the notification requirements in subsection (b) to the source named in the recommendation, Congress, and the Office of Management and Budget, and still make a determination to exclude a source under subsection (b)(4) if there is an urgent national security reason for an immediate use of the authorities in subsection (a). Once the national security issue has been addressed, the DHS Secretary must take action to complete the notification requirements.

Subsection (d) requires the Secretary to review all of the exclusion determinations made pursuant to subsection (b) on an annual basis.

Subsection (e) prohibits the Secretary from delegating the authority in subsection (a) or subsection (d) to any Departmental official below the Deputy Secretary level.

Subsection (f) exempts any action taken under subsection (a) from review under a bid protest through the Government Accountability Office or in Federal court.

Subsection (g) requires the Secretary to review similar procedures and guidelines used by the Department of Defense when developing the procedures and guidelines for the Department of Homeland Security.

Subsection (h) defines the following terms: "covered article," "covered procurement," "covered procurement action," "information technology," "responsible source," "supply chain risk,"

"telecommunications equipment," and "telecommunications service."

Subsection (i) sets 90 days after enactment as the effective date for the authorities described in this section. In addition, this section exempts the Secretary from public notice and meeting requirements related to the Federal rulemaking procedures established under section 553 of Title 5 and section 1707 of Title 41.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italic and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

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

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

* * * * * * *

Subtitle D—Acquisitions

* * * * * * *

SEC. 836. REQUIREMENTS FOR INFORMATION RELATING TO SUPPLY CHAIN RISK.

(a) AUTHORITY.—Subject to subsection (b), the Secretary may—

(1) carry out a covered procurement action;

(2) limit, notwithstanding any other provision of law, in whole or in part, the disclosure of information, including classified information, relating to the basis for carrying out such an action; and

(3) exclude, in whole or in part, a source carried out in the course of such an action applicable to a covered procurement of the Department.

(b) DETERMINATION AND NOTIFICATION.—Except as authorized by subsection (c) to address an urgent national security interest, the Secretary 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 Department, including a review of any risk assessment made available by an appropriate person or entity, including the national risk management center at the Cybersecurity and Infrastructure Security Agency, that there is a significant supply chain risk in a covered procurement;

(2) notifying any source named in the joint recommendation described in paragraph (1) advising—

(A) that a recommendation has been obtained;

(B) to the extent consistent with the national security and law enforcement interests, the basis for such recommendation;

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

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

(3) notifying the relevant components of the Department that such risk assessment has demonstrated significant supply chain risk to a covered procurement;

(4) making a determination in writing, in unclassified or classified form, that after considering any information submitted by a source under paragraph (2), and in consultation with the Chief Information Officer of the Department, that—

(A) use of authority under subsection (a)(1) is necessary to protect national security by reducing supply chain risk;

(B) less intrusive measures are not reasonably available to reduce such risk;

(C) a decision to limit disclosure of information under subsection (a)(2) is necessary to protect national security interest; and

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

(5) providing to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a classified or unclassified notice of the determination made under paragraph (4) that includes—

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

(B) a summary of any risk assessment reviewed in support of such joint recommendation; and

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

(6) notifying the Director of the Office of Management and Budget, and the heads of other Federal agencies as appropriate, in a manner and to the extent consistent with the requirements of national security; and

(7) taking steps to maintain the confidentiality of any notifications under this subsection.

(c) PROCEDURES TO ADDRESS URGENT NATIONAL SECURITY INTERESTS.—In any case in which the Secretary determines that national security interests require the immediate exercise of the authorities under subsection (a), the Secretary—

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

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

(B) make the determination required by subsection (b)(4), regardless of whether the notice required by subsection (b)(2) has been provided or whether the notified source at issue has submitted any information in response to such notice;

(C) temporarily delay the notice required by subsections (b)(4) and (b)(5); and

(D) exercise the authority provided in subsection (a) in accordance with such determination; 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 that is the subject of paragraph (1), including—

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

(B) promptly considering any information submitted by the source at issue in response to such notice, and making any appropriate modifications to the determination required by subsection (b)(4) based on such information; and

(C) providing the notice required by subsections (b)(5) and (b)(6), including a description of such urgent national security, and any modifications to such determination made in accordance with subparagraph (B).

(d) ANNUAL REVIEW OF DETERMINATIONS.—The Secretary shall annually review all determinations made under subsection (b).

(e) DELEGATION.—The Secretary may not delegate the authority provided in subsection (a) or the responsibility identified in subsection (d) to an official below the Deputy Secretary.

(f) LIMITATION OF REVIEW.—Notwithstanding any other provision of law, no action taken by the Secretary under subsection (a) may be subject to review in a bid protest before the Government Accountability Office or in any Federal court.

(g) CONSULTATION.—In developing procedures and guidelines for the implementation of the authorities described in this section, the Secretary shall review the procedures and guidelines utilized by the Department of Defense to carry out similar authorities.

(h) DEFINITIONS.—In this section:

(1) COVERED ARTICLE.—The term "covered article" means:

(A) Information technology, including cloud computing services of all types.

(B) Telecommunications equipment.

(C) Telecommunications services.

(D) The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program of the Department.

(E) Hardware, systems, devices, software, or services that include embedded or incidental information technology.

(2) 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 title 41, United States Code, or an evaluation factor, as provided in subsection (c)(1)(A) of such section, relating to supply chain risk, or with respect to which supply chain risk considerations are included in the Department's determination of whether a source is a responsible source as defined in section 113 of such 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 title 41, United States Code, with respect to which the task or delivery order contract includes a contract clause establishing a requirement relating to supply chain risk;

(C) any contract action involving a contract for a covered article with respect to which such contract includes a clause establishing requirements relating to supply chain risk; or

(D) any procurement made via Government Purchase Care for a covered article when supply chain risk has been identified as a concern.

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

(A) The exclusion of a source that fails to meet qualification requirements established pursuant to section 3311 of title 41, United States Code, for the purpose of reducing supply chain risk in the acquisition or use of a covered article.

(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 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.

(4) INFORMATION SYSTEM.—The term "information system" has the meaning given such term in section 3502 of title 44, United States Code.

(5) INFORMATION TECHNOLOGY.—The term "information technology" has the meaning given such term in section 11101 of title 40, United States Code.

(6) RESPONSIBLE SOURCE.—The term "responsible source" has the meaning given such term in section 113 of title 41, United States Code.

(7) SUPPLY CHAIN RISK.—The term "supply chain risk" means the risk that a malicious actor may sabotage, maliciously introduce an unwanted function, extract or modify data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered article so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the information technology or information stored or transmitted on the covered articles.

(8) TELECOMMUNICATIONS EQUIPMENT.—The term "telecommunications equipment" has the meaning given such term in section 3(52) of the Communications Act of 1934 (47 U.S.C. 153(52)).

(9) TELECOMMUNICATIONS SERVICE.—The term "telecommunications service" has the meaning given such term in section 3(53) of the Communications Act of 1934 (47 U.S.C. 153(53)).

(i) EFFECTIVE DATE.—The requirements of 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—

(1) contracts awarded on or after such date; and

(2) task and delivery orders issued on or after such date pursuant to contracts awarded before, on, or after such date.

* * * * * * *

○