117TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
117–120

DHS SOFTWARE SUPPLY CHAIN RISK MANAGEMENT ACT OF 2021

SEPTEMBER 14, 2021.—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. 4611]

The Committee on Homeland Security, to whom was referred the bill (H.R. 4611) to direct the Secretary of Homeland Security to issue guidance with respect to certain information and communications technology or services contracts, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends 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 "DHS Software Supply Chain Risk Management Act of 2021".

SEC. 2. DEPARTMENT OF HOMELAND SECURITY GUIDANCE WITH RESPECT TO CERTAIN INFORMATION AND COMMUNICATIONS TECHNOLOGY OR SERVICES CONTRACTS.

(a) GUIDANCE.—The Secretary of Homeland Security, acting through the Under Secretary, shall issue guidance with respect to new and existing covered contracts.

(b) NEW COVERED CONTRACTS.—In developing guidance under subsection (a), with respect to each new covered contract, as a condition on the award of such a contract, each contractor responding to a solicitation for such a contract shall submit to the covered officer—

(1) a planned bill of materials when submitting a bid proposal; and

(2) the certification and notifications described in subsection (e).

(c) EXISTING COVERED CONTRACTS.—In developing guidance under subsection (a), with respect to each existing covered contract, each contractor with an existing covered contract shall submit to the covered officer—

(1) the bill of materials used for such contract, upon the request of such officer; and

(2) the certification and notifications described in subsection (e).

(d) UPDATING BILL OF MATERIALS.—With respect to a covered contract, in the case of a change to the information included in a bill of materials submitted pursuant to subsections (b)(1) and (c)(1), each contractor shall submit to the covered officer the update to such bill of materials, in a timely manner.

(e) CERTIFICATION AND NOTIFICATIONS.—The certification and notifications referred to in subsections (b)(2) and (c)(2), with respect to a covered contract, are the following:

(1) A certification that each item listed on the submitted bill of materials is free from all known vulnerabilities or defects affecting the security of the end product or service identified in—

(A) the National Institute of Standards and Technology National Vulnerability Database; and

(B) any database designated by the Under Secretary, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, that tracks security vulnerabilities and defects in open source or third-party developed software.

(2) A notification of each vulnerability or defect affecting the security of the end product or service, if identified, through—

(A) the certification of such submitted bill of materials required under paragraph (1); or

(B) any other manner of identification.

(3) A notification relating to the plan to mitigate, repair, or resolve each security vulnerability or defect listed in the notification required under paragraph (2).

(f) ENFORCEMENT.—In developing guidance under subsection (a), the Secretary shall instruct covered officers with respect to—

(1) the processes available to such officers enforcing subsections (b) and (c); and

(2) when such processes should be used.

(g) EFFECTIVE DATE.—The guidance required under subsection (a) shall take effect on the date that is 180 days after the date of the enactment of this section.

(h) GAO REPORT.—Not later than 1 year after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Secretary, the Committee on Homeland Security of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate a report that includes—

(1) a review of the implementation of this section;

(2) information relating to the engagement of the Department of Homeland Security with industry;

(3) an assessment of how the guidance issued pursuant to subsection (a) complies with Executive Order 14208 (86 Fed. Reg. 26633; relating to improving the nation's cybersecurity); and

(4) any recommendations relating to improving the supply chain with respect to covered contracts.

(i) DEFINITIONS.—In this section:

(1) BILL OF MATERIALS.—The term "bill of materials" means a list of the parts and components (whether new or reused) of an end product or service, including, with respect to each part and component, information relating to the origin, composition, integrity, and any other information as determined appropriate by the Under Secretary.

(2) COVERED CONTRACT.—The term "covered contract" means a contract relating to the procurement of covered information and communications technology or services for the Department of Homeland Security.

(3) COVERED INFORMATION AND COMMUNICATIONS TECHNOLOGY OR SERVICES.—The term "covered information and communications technology or services" means the terms—

(A) "information technology" (as such term is defined in section 11101(6) of title 40, United States Code);

(B) "information system" (as such term is defined in section 3502(8) of title 44, United States Code);

(C) "telecommunications equipment" (as such term is defined in section 3(52) of the Communications Act of 1934 (47 U.S.C. 153(52))); and

(D) "telecommunications service" (as such term is defined in section 3(53) of the Communications Act of 1934 (47 U.S.C. 153(53))).

(4) COVERED OFFICER.—The term "covered officer" means—

(A) a contracting officer of the Department; and

(B) any other official of the Department as determined appropriate by the Under Secretary.

(5) SOFTWARE.—The term "software" means computer programs and associated data that may be dynamically written or modified during execution.

(6) UNDER SECRETARY.—The term "Under Secretary" means the Under Secretary for Management of the Department of Homeland Security.

PURPOSE AND SUMMARY

H.R. 4611, the "DHS Software Supply Chain Risk Management Act of 2021," seeks to enhance the Department of Homeland Security's (DHS) ability to protect its networks from malicious cyberattacks by modernizing how the Department procures information and communications technology or services (ICT(S)). The bill would require the Under Secretary for Management (USM) to issue Department-wide guidance to improve DHS's insight into the software it purchases from new and existing ICT(S) contractors. Specifically, contractors are to provide DHS with a software bill of materials that identifies key information, such as the origin of each part or component of new or reused software supplied to the Department. Contractors are also required to certify that each item listed on the software bill of materials is free from all known vulnerabilities or defects that affect the security of supplied ICT(S) capabilities and to notify DHS of any identified issues and plans for addressing them. The Comptroller General, in turn, is required to report to Congress on DHS's implementation of the guidance required by this Act, engagement with industry, and compliance with Executive Order 14208 related to improving the Nation's cybersecurity, among other things.

BACKGROUND AND NEED FOR LEGISLATION

Cyberattacks against the United States are becoming increasingly more frequent and sophisticated, posing a significant threat to homeland security and the U.S. economy. The SolarWinds cyber espionage campaign discovered in 2020 demonstrated that the Federal Government is not immune to such attacks. During this campaign, hackers were able to add malicious code to a commercial software product that was downloaded by several Federal agencies, including DHS, and gain unfettered access inside Federal information systems.

Unfortunately, the SolarWinds cyber espionage campaign was not the first to compromise sensitive software supply chains. The Atlantic Council identified 115 instances, since 2010, of publicly re-

ported attacks on the software supply chain or disclosure of high-impact vulnerabilities likely to be exploited in such attacks.[1]

As the lead Federal agency for cybersecurity, DHS's Cybersecurity and Infrastructure Security Agency (CISA) has taken steps to increase awareness of the top vulnerabilities routinely exploited by malicious cyber actors.[2] To identify and manage these types of vulnerabilities on its own networks, DHS needs visibility into the supply chains of the ICT(S) capabilities it procures in support of the Department's many missions. The guidance required by the "DHS Software Supply Chain Risk Management Act of 2021" would assure such visibility.

The Committee recognizes H.R. 4611 places new requirements on industry. As DHS develops the guidance, the Department may consider phasing-in the requirements for small businesses and prioritizing existing ICT(S) contracts that are high-risk or high-value. Ultimately, full implementation of the requirements regardless of contractor type or size is necessary for DHS to effectively manage potential cyber threats facing the Department.

HEARINGS

For the purposes of clause 3(c)(6) of rule XIII of the Rules of the House of Representatives, the following hearings were used to develop H.R. 4611:

On February 10, 2021, the Committee held a hearing entitled "Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience." The Committee received testimony from Mr. Chris Krebs, former Director of the Cybersecurity and Infrastructure Security Agency, DHS; Ms. Sue Gordon, former Principal Deputy Director of National Intelligence, Office of the Director of National Intelligence; Mr. Michael Daniel, President and Chief Executive Officer, Cyber Threat Alliance; and Mr. Dmitri Alperovitch, Executive Chairman, Silverado Policy Accelerator.

On February 26, 2021, the Committee held a hearing entitled "Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and the Ongoing Campaign." The Committee received testimony from Mr. Sudhakar Ramakrishna, President and Chief Executive Officer, SolarWinds Corporation; Mr. Kevin B. Thompson, former Chief Executive Officer, SolarWinds Corporation; Mr. Kevin Mandia, Chief Executive Officer, FireEye, Inc.; Mr. Bradford L. Smith, President and Chief Legal Officer, Microsoft Corporation.

COMMITTEE CONSIDERATION

The Committee met on July 28, 2021, a quorum being present, to consider H.R. 4611 and ordered the measure to be favorably reported to the House, as amended, by voice vote.

---

[1] Dr. Trey Herr, William Loomis, Stewart Scott, and June Lee, *Breaking Trust: Shades of Crisis across an Insecure Software Supply Chain*, Atlantic Council, (July 26, 2020), Available at https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/.

[2] Cybersecurity and Infrastructure Security Agency, "Top Routinely Exploited Vulnerabilities," *Alert (AA21–209A)*, (July 28, 2020), Available at https://us-cert.cisa.gov/ncas/alerts/aa21-209a.

COMMITTEE VOTES

Clause 3(b) of rule XIII 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. 4611.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X, 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 and section 308(a) of the Congressional Budget Act of 1974, and with respect to the requirements of clause 3(c)(3) of rule XIII and section 402 of the Congressional Budget Act of 1974, the Committee has requested but not received from the Director of the Congressional Budget Office a statement as to whether this bill contains any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures.

FEDERAL MANDATES STATEMENT

An estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the Congressional Record upon its receipt by the Committee.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 4611 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the objective of H.R. 4611 is to enhance DHS's ability to protect its networks from malicious cyberattacks by improving the Department's insight into the software purchased for ICT(S) in support of its management and operational functions.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS ADVISORY COMMITTEE STATEMENT

In compliance with rule XXI, 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 rule XXI.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that H.R. 4611 does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short Title.

This section states that the Act may be cited as the "DHS Software Supply Chain Risk Management Act of 2021".

Sec. 2. Department of Homeland Security Guidance with Respect to Certain Information and Communications Technology or Services Contracts.

Subsection 2(a) directs the Secretary of Homeland Security, acting through the USM, to issue guidance with respect to new and existing covered ICT(S) contracts.

Subsection 2(b) outlines what content the USM's guidance is to include related to new covered contracts. Specifically, the guidance requires that, as a condition for the award of a new ICT(S) contract, each contractor submits a planned bill of materials as a part of its bid proposal and the certifications and notifications described in subsection 2(e).

Subsection 2(c) outlines what content the guidance is to include related to existing covered contracts. Specifically, the guidance requires that, at the request of the Department, an existing ICT(S) contractor submit a bill of materials and the certifications and notifications described in subsection 2(e).

Subsection 2(d) directs new or existing contractors to provide the Department with an updated bill of materials in a timely manner if any changes are made subsequent to a bill of materials having already been submitted to the Department.

Subsection 2(e) outlines the certification and notification requirements new and existing contractors are to make with respect to covered ICT(S) contracts. Specifically, contractors are required to provide a certification to the Department that each item listed on a submitted bill of materials is free from all known vulnerabilities or defects affecting the security of the end product or service supplied to DHS. In doing so, contractors are required to consult the National Institute of Standards and Technology National Vulnerability Database and any other database identified by the USM, in coordination with the Director of CISA, that tracks security vulnerabilities and defects in open source or third-party developed software. Contractors are required to provide a notification to the Department of each vulnerability or defect affecting the security of the end product or service supplied to DHS identified through the certification process or any other manner. Additionally, contractors are to provide a notification to the Department outlining how they will mitigate, repair, or resolve each identified vulnerability or defect.

Subsection 2(f) directs the Secretary to include instructions in the guidance related to how and when Department officials are to enforce the requirements outlined in the guidance for new and existing covered contracts.

Subsection 2(g) establishes that the guidance is to take effect 180 days after the enactment of the section.

Subsection 2(h) directs the Comptroller General of the United States to submit a report to Congress no later than 1 year after the enactment of the Act. The report is to include a review of DHS's implementation of the requirements outlined in the Act; information related to DHS's engagement with industry; an assessment of how the Department's guidance complies with Executive Order 14208 related to improving the Nation's cybersecurity; and any recommendations related to improving the supply chain with respect to covered ICT(S) contracts.

Subsection 2(i) defines key terms, including "bill of materials," "covered contract," "covered information and communications technology or services," and "software."

○