I

113TH CONGRESS
2D SESSION

H. R. 5793

To ensure the integrity of any software, firmware, or product developed for or purchased by the United States Government that uses a third party or open source component, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 4, 2014

Mr. ROYCE (for himself and Ms. JENKINS) introduced the following bill; which was referred to the Committee on Oversight and Government Reform

---

A BILL

To ensure the integrity of any software, firmware, or product developed for or purchased by the United States Government that uses a third party or open source component, 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.

This Act may be cited as the ''Cyber Supply Chain Management and Transparency Act of 2014''.

SEC. 2. SOFTWARE, FIRMWARE, OR PRODUCT WITH KNOWN SECURITY VULNERABILITIES OR DEFECTS.

(a) OMB GUIDELINES REQUIRED.—

(1) CLAUSES REQUIRED IN SOFTWARE, FIRMWARE, OR PRODUCT CONTRACTS FOR SOFTWARE, FIRMWARE, OR PRODUCT CREATED WITH A BINARY COMPONENT.—Not later than 180 days after the date of the enactment of this Act, the Director of the Office of Management and Budget, in consultation with the Secretary of Defense, the Secretary of Homeland Security, and any other intelligence or national security agency the Director determines to be necessary, shall issue guidelines for each agency that require including the following clauses in any contract for the acquisition of software, firmware, or product that contains a binary component:

(A) COMPONENT LIST.—A clause that requires the inclusion of a comprehensive and confidentially supplied list, or a bill of materials, of each binary component of the software, firmware, or product that is used in the software, firmware, or product.

(B) VERIFICATION REQUIRED.—A clause that requires the contractor providing the software, firmware, or product—

(i) to verify that the software, firmware, or product does not contain any

known security vulnerabilities or defects that are listed in the National Institute of Standards and Technology National Vulnerability Database and any additional database selected by the Director of the Office of Management and Budget (that is credible and similar to the National Vulnerability Database) that tracks security vulnerabilities and defects in a binary component, and that is necessary to capture a wider list of binary components (with known security vulnerabilities or defects and for which a less vulnerable alternative is available); and

(ii) to notify the purchasing agency of any known security vulnerabilities or defects discovered through the verification required under clause (i).

(C) WAIVER.—A clause that requires—

(i) a contractor to submit a written application, and obtain a waiver, for each binary component that is known to be vulnerable from the head of the purchasing agency; and

(ii) if the head of the purchasing agency approves the waiver, such head shall provide the contractor with a written statement that the agency accepts all of the risk associated with the use of such binary component.

(D) UPDATES.—A clause that requires such software, firmware, or product to be written or designed in a manner that allows for any future security vulnerability or defect in any part of the software, firmware, or product to be easily patched, updated, or replaced to fix the vulnerability or defect in the software, firmware, or product.

(E) TIMELY REPAIR.—A clause that requires the contractor to provide a repair in a timely manner with regard to any new security vulnerability discovered through any of the databases described in subparagraph (B).

(2) DISCLOSURE OF SECURITY VULNERABILITY OR DEFECT.—Not later than 180 days after the date of the enactment of this Act, the Director of the Office of Management and Budget shall issue guidelines for each agency with respect to any software, firmware, or product in use by the United States

Government that contains a binary component that requires each agency to have a process—

(A) to replace any currently known vulnerable binary component; and

(B) to remove and repair any new vulnerable binary component after such component becomes known pursuant to paragraph (1)(B).

(3) AGENCY GUIDELINES.—

(A) SOFTWARE, FIRMWARE, OR PRODUCT THAT CAN NOT BE FIXED OR PATCHED.—Not later than 220 days after the date of the enactment of this Act, the Director of the Office of Management and Budget shall issue guidelines for each agency with respect to any software, firmware, or product that contains a known vulnerable binary component—

(i) that can not be fixed, patched, or updated; and

(ii) that requires such component, to migrate to patchable, repairable, and fixable products.

(B) INVENTORY OF EXISTING SOFTWARE, FIRMWARE, OR PRODUCT WITH A KNOWN VULNERABLE BINARY COMPONENT.—Not later than 20 months after the date of the enactment of

this Act, the Director of the Office of Budget of Management shall instruct each agency to provide the relevant office in the Department of Homeland Security with a list of each known vulnerable binary in any software, firmware or product in use by each agency.

(C) ANALYSIS OF PROJECT INTEGRITY AND ANNUAL REPORT.—Not later than twelve months after all lists described in subparagraph (B) are provided to the Department of Homeland Security, the Secretary of Homeland Security shall issue an annual confidential report describing the security vulnerabilities of the projects that created any known vulnerable binary component in any list described in subparagraph (B) and through the verification required under paragraph (1)(B). The report shall assess the integrity of binary component suppliers for the incidence of security vulnerabilities, the severity, the mean time to remediate such vulnerabilities that can be applied to assess the security of binary projects and suppliers, for use by other agencies.

(b) REPORT ON REMOVAL OF BINARY COMPONENT WITH KNOWN SECURITY VULNERABILITY OR DEFECT.—

Not later than 30 months after the date of the enactment of this Act, the head of each agency shall submit to each relevant Committee of jurisdiction in the House of Representatives and the Senate a report on the completion of the removal of each binary component with known security vulnerabilities or defects in the agency and shall include a classified version of this report for the Permanent Select Committee on Intelligence and the Committees on Armed Services, Foreign Affairs, and Homeland Security of the House of Representatives and the Select Committee on Intelligence and the Committees on Armed Services, Foreign Affairs, and Homeland Security and Governmental Affairs of the Senate. The report shall also detail the policies, procedures, and processes by which a newly discovered vulnerable binary component is replaced in software, firmware, and products in use by the United States Government.

(c) OTHER ENTITIES OF THE UNITED STATES GOVERNMENT.—Any other entity of the United States Government—

(1) shall replace any vulnerable binary component with another less vulnerable alternative in any software, firmware, or product in use by the entity; and

(2) shall begin such replacement process with critical systems.

(d) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''agency'' has the meaning given that term in section 551(1) of title 5, United States Code.

(2) BINARY COMPONENT.—The term ''binary component'' means a third party or open source component.

○