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.

1 *Be it enacted by the Senate and House of Representa-*

2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4   This Act may be cited as the "Cyber Supply Chain

5 Management and Transparency Act of 2014".

6 **SEC. 2. SOFTWARE, FIRMWARE, OR PRODUCT WITH KNOWN**

7   **SECURITY VULNERABILITIES OR DEFECTS.**

8   (a) OMB GUIDELINES REQUIRED.—

1 　　　(1) CLAUSES REQUIRED IN SOFTWARE,

2 FIRMWARE, OR PRODUCT CONTRACTS FOR SOFT-

3 WARE, FIRMWARE, OR PRODUCT CREATED WITH A

4 BINARY COMPONENT.—Not later than 180 days

5 after the date of the enactment of this Act, the Di-

6 rector of the Office of Management and Budget, in

7 consultation with the Secretary of Defense, the Sec-

8 retary of Homeland Security, and any other intel-

9 ligence or national security agency the Director de-

10 termines to be necessary, shall issue guidelines for

11 each agency that require including the following

12 clauses in any contract for the acquisition of soft-

13 ware, firmware, or product that contains a binary

14 component:

15 　　　　　(A) COMPONENT LIST.—A clause that re-

16 quires the inclusion of a comprehensive and

17 confidentially supplied list, or a bill of mate-

18 rials, of each binary component of the software,

19 firmware, or product that is used in the soft-

20 ware, firmware, or product.

21 　　　　　(B) VERIFICATION REQUIRED.—A clause

22 that requires the contractor providing the soft-

23 ware, firmware, or product—

24 　　　　　　　(i) to verify that the software,

25 firmware, or product does not contain any

1 known security vulnerabilities or defects
2 that are listed in the National Institute of
3 Standards and Technology National Vul-
4 nerability Database and any additional
5 database selected by the Director of the
6 Office of Management and Budget (that is
7 credible and similar to the National Vul-
8 nerability Database) that tracks security
9 vulnerabilities and defects in a binary com-
10 ponent, and that is necessary to capture a
11 wider list of binary components (with
12 known security vulnerabilities or defects
13 and for which a less vulnerable alternative
14 is available); and

15 (ii) to notify the purchasing agency of
16 any known security vulnerabilities or de-
17 fects discovered through the verification re-
18 quired under clause (i).

19 (C) WAIVER.—A clause that requires—

20 (i) a contractor to submit a written
21 application, and obtain a waiver, for each
22 binary component that is known to be vul-
23 nerable from the head of the purchasing
24 agency; and

1   (ii) if the head of the purchasing

2   agency approves the waiver, such head

3   shall provide the contractor with a written

4   statement that the agency accepts all of

5   the risk associated with the use of such bi-

6   nary component.

7   (D) UPDATES.—A clause that requires

8   such software, firmware, or product to be writ-

9   ten or designed in a manner that allows for any

10   future security vulnerability or defect in any

11   part of the software, firmware, or product to be

12   easily patched, updated, or replaced to fix the

13   vulnerability or defect in the software,

14   firmware, or product.

15   (E) TIMELY REPAIR.—A clause that re-

16   quires the contractor to provide a repair in a

17   timely manner with regard to any new security

18   vulnerability discovered through any of the

19   databases described in subparagraph (B).

20   (2) DISCLOSURE OF SECURITY VULNERABILITY

21   OR DEFECT.—Not later than 180 days after the date

22   of the enactment of this Act, the Director of the Of-

23   fice of Management and Budget shall issue guide-

24   lines for each agency with respect to any software,

25   firmware, or product in use by the United States

1   Government that contains a binary component that

2   requires each agency to have a process—

3   (A) to replace any currently known vulner-

4   able binary component; and

5   (B) to remove and repair any new vulner-

6   able binary component after such component

7   becomes known pursuant to paragraph (1)(B).

8   (3) AGENCY GUIDELINES.—

9   (A) SOFTWARE, FIRMWARE, OR PRODUCT

10   THAT CAN NOT BE FIXED OR PATCHED.—Not

11   later than 220 days after the date of the enact-

12   ment of this Act, the Director of the Office of

13   Management and Budget shall issue guidelines

14   for each agency with respect to any software,

15   firmware, or product that contains a known vul-

16   nerable binary component—

17   (i) that can not be fixed, patched, or

18   updated; and

19   (ii) that requires such component, to

20   migrate to patchable, repairable, and fix-

21   able products.

22   (B) INVENTORY OF EXISTING SOFTWARE,

23   FIRMWARE, OR PRODUCT WITH A KNOWN VUL-

24   NERABLE BINARY COMPONENT.—Not later than

25   20 months after the date of the enactment of

1   this Act, the Director of the Office of Budget

2   of Management shall instruct each agency to

3   provide the relevant office in the Department of

4   Homeland Security with a list of each known

5   vulnerable binary in any software, firmware or

6   product in use by each agency.

7   (C) ANALYSIS OF PROJECT INTEGRITY

8   AND ANNUAL REPORT.—Not later than twelve

9   months after all lists described in subparagraph

10   (B) are provided to the Department of Home-

11   land Security, the Secretary of Homeland Secu-

12   rity shall issue an annual confidential report de-

13   scribing the security vulnerabilities of the

14   projects that created any known vulnerable bi-

15   nary component in any list described in sub-

16   paragraph (B) and through the verification re-

17   quired under paragraph (1)(B). The report

18   shall assess the integrity of binary component

19   suppliers for the incidence of security

20   vulnerabilities, the severity, the mean time to

21   remediate such vulnerabilities that can be ap-

22   plied to assess the security of binary projects

23   and suppliers, for use by other agencies.

24   (b) REPORT ON REMOVAL OF BINARY COMPONENT

25 WITH KNOWN SECURITY VULNERABILITY OR DEFECT.—

1 Not later than 30 months after the date of the enactment

2 of this Act, the head of each agency shall submit to each

3 relevant Committee of jurisdiction in the House of Rep-

4 resentatives and the Senate a report on the completion

5 of the removal of each binary component with known secu-

6 rity vulnerabilities or defects in the agency and shall in-

7 clude a classified version of this report for the Permanent

8 Select Committee on Intelligence and the Committees on

9 Armed Services, Foreign Affairs, and Homeland Security

10 of the House of Representatives and the Select Committee

11 on Intelligence and the Committees on Armed Services,

12 Foreign Affairs, and Homeland Security and Govern-

13 mental Affairs of the Senate. The report shall also detail

14 the policies, procedures, and processes by which a newly

15 discovered vulnerable binary component is replaced in soft-

16 ware, firmware, and products in use by the United States

17 Government.

18 (c) OTHER ENTITIES OF THE UNITED STATES GOV-

19 ERNMENT.—Any other entity of the United States Gov-

20 ernment—

21   (1) shall replace any vulnerable binary compo-

22   nent with another less vulnerable alternative in any

23   software, firmware, or product in use by the entity;

24   and

1   (2) shall begin such replacement process with

2   critical systems.

3   (d) DEFINITIONS.—In this section:

4   (1) AGENCY.—The term "agency" has the

5   meaning given that term in section 551(1) of title 5,

6   United States Code.

7   (2) BINARY COMPONENT.—The term "binary

8   component" means a third party or open source

9   component.

○