II

Calendar No. 76

118TH CONGRESS
1ST SESSION

S. 917

[Report No. 118–32]

To establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software security, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MARCH 22, 2023

Mr. PETERS (for himself and Mr. HAWLEY) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

MAY 16, 2023

Reported by Mr. PETERS, with amendments

[Omit the part struck through and insert the part printed in italic]

A BILL

To establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software 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.

This Act may be cited as the ‘‘Securing Open Source Software Act of 2023’’.

SEC. 2. FINDINGS.

Congress finds that—

(1) open source software fosters technology development and is an integral part of overall cybersecurity;

(2) a secure, healthy, vibrant, and resilient open source software ecosystem is crucial for ensuring the national security and economic vitality of the United States;

(3) open source software is part of the foundation of digital infrastructure that promotes a free and open internet;

(4) due to both the unique strengths of open source software and inconsistent historical investment in open source software security, there exist unique challenges in securing open source software; and

(5) the Federal Government should play a supporting role in ensuring the long-term security of open source software.

SEC. 3. OPEN SOURCE SOFTWARE SECURITY DUTIES.

(a) IN GENERAL.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 650 et seq.) is amended—

(1) in section 2200 (6 U.S.C. 650)—

(A) by redesignating paragraphs (22) through (28) as paragraphs (25) through (31), respectively; and

(B) by inserting after paragraph (21) the following:

"(22) OPEN SOURCE SOFTWARE.—The term 'open source software' means software for which the human-readable source code is made available to the public for use, study, re-use, modification, enhancement, and re-distribution.

"(23) OPEN SOURCE SOFTWARE COMMUNITY.—The term 'open source software community' means the community of individuals, foundations, nonprofit organizations, corporations, and other entities that—

"(A) develop, contribute to, maintain, and publish open source software; or

"(B) otherwise work to ensure the security of the open source software ecosystem.

"(24) OPEN SOURCE SOFTWARE COMPONENT.—The term 'open source software component' means an individual repository of open source software that is made available to the public.";

(2) in section 2202(c) (6 U.S.C. 652(c))—

(A) in paragraph (13), by striking ''and'' at the end;

(B) by redesignating paragraph (14) as paragraph (15); and

(C) by inserting after paragraph (13) the following:

''(14) support, including by offering services, the secure usage and deployment of software, including open source software, in the software development lifecycle at Federal agencies in accordance with section ~~2220E~~ *section 2220F*; and''; and

(3) by adding at the end the following:

''SEC. 2220F. OPEN SOURCE SOFTWARE SECURITY DUTIES.

''(a) DEFINITION.—In this section, the term 'software bill of materials' has the meaning given the term in the Minimum Elements for a Software Bill of Materials published by the Department of Commerce, or any superseding definition published by the Agency.

''(b) EMPLOYMENT.—The Director shall, to the greatest extent practicable, employ individuals in the Agency who—

''(1) have expertise and experience participating in the open source software community; and

''(2) perform the duties described in subsection (c).

''(c) DUTIES OF THE DIRECTOR.—

''(1) IN GENERAL.—The Director shall—

''(A) perform outreach and engagement to bolster the security of open source software;

''(B) support Federal efforts to strengthen the security of open source software;

''(C) coordinate, as appropriate, with non-Federal entities on efforts to ensure the long-term security of open source software;

''(D) serve as a public point of contact regarding the security of open source software for non-Federal entities, including State, local, Tribal, and territorial partners, the private sector, international partners, ~~open source software organizations, and open source software developers~~ *and the open source software community*; and

''(E) support Federal and non-Federal supply chain security efforts by encouraging efforts to bolster open source software security, such as—

''(i) assisting in coordinated vulnerability disclosures in open source software components pursuant to section 2209(n); and "(ii) supporting the activities of the Federal Acquisition Security Council.

"(2) ASSESSMENT OF CRITICAL OPEN SOURCE SOFTWARE COMPONENTS.—

"(A) FRAMEWORK.—Not later than 1 year after the date of enactment of this section, the Director shall publicly publish a framework, incorporating government, industry, and open source software community frameworks and best practices, including those published by the National Institute of Standards and Technology, for assessing the risk of open source software components, including direct and indirect open source software dependencies, which shall incorporate, at a minimum—

"(i) the security properties of code in a given open source software component, such as whether the code is written in a memory-safe programming language;

"(ii) the security practices of development, build, and release processes of a given open source software component, such as the use of multi-factor authentication by maintainers and cryptographic signing of releases;

''(iii) the number and severity of publicly known, unpatched vulnerabilities in a given open source software component;

''(iv) the breadth of deployment of a given open source software component;

''(v) the level of risk associated with where a given open source software component is integrated or deployed, such as whether the component operates on a network boundary or in a privileged location; and

''(vi) the health of the *open source software* community for a given open source software component, including, where applicable, the level of current and historical investment and maintenance in the open source software component, such as the number and activity of individual maintainers.

''(B) UPDATING FRAMEWORK.—Not less frequently than annually after the date on which the framework is published under subparagraph (A), the Director shall—

''(i) determine whether updates are needed to the framework described in subparagraph (A), including the augmentation, addition, or removal of the elements described in clauses (i) through (vi) of such subparagraph; and

"(ii) if the Director determines that additional updates are needed under clause (i), make those updates to the framework.

"(C) Developing framework.—In developing the framework described in subparagraph (A), the Director shall consult with—

"(i) appropriate Federal agencies, including the National Institute of Standards and Technology;

"(ii) individuals and nonprofit organizations from the open source software community; and

"(iii) private companies from the open source software community.

"(D) Usability.—The Director shall ensure, to the greatest extent practicable, that the framework described in subparagraph (A) is usable by the open source software community, including through the consultation described in subparagraph (C).

"(E) Federal open source software assessment.—Not later than 1 year after the publication of the framework described in subparagraph (A), and not less frequently than every 2 years thereafter, the Director shall, to the greatest extent practicable and using the framework described in subparagraph (A)—

"(i) perform an assessment of open source software components used directly or indirectly by Federal agencies based on readily available, and, to the greatest extent practicable, machine readable, information, such as—

"(I) software bills of materials that are, at the time of the assessment, made available to the Agency or are otherwise accessible via the internet;

"(II) software inventories, available to the Director at the time of the assessment, from the Continuous Diagnostics and Mitigation program of the Agency; and

"(III) other publicly available information regarding open source software components; and

"(ii) develop 1 or more ranked lists of components described in clause (i) based on the assessment, such as ranked by the criticality, level of risk, or usage of the components, or a combination thereof.

"(F) AUTOMATION.—The Director shall, to the greatest extent practicable, automate the assessment conducted under subparagraph (E).

"(G) PUBLICATION.—The Director shall publicly publish and maintain any tools developed to conduct the assessment described in subparagraph (E) as open source software.

"(H) SHARING.—

"(i) RESULTS.—The Director shall facilitate the sharing of the results of ~~the~~ *each* assessment described in subparagraph (E) *(i)* with appropriate Federal and non-Federal entities working to support the security of open source software, including by offering means for appropriate Federal and non-Federal entities to download the assessment in an automated manner.

"(ii) DATASETS.—The Director may publicly publish, as appropriate, any datasets or versions of the datasets developed or consolidated as a result of ~~the~~ *an* assessment described in subparagraph (E) *(i)*.

"(I) CRITICAL INFRASTRUCTURE ASSESSMENT STUDY AND PILOT.—

"(i) STUDY.—Not later than 2 years after the publication of the framework described in subparagraph (A), the Director shall conduct a study regarding the feasibility of the Director conducting the assessment described in subparagraph (E) for critical infrastructure entities.

"(ii) PILOT.—

"(I) IN GENERAL.—If the Director determines that the assessment described in clause (i) is feasible, the Director may conduct a pilot assessment on a voluntary basis with 1 or more critical infrastructure sectors, in coordination with the Sector Risk Management Agency and the sector coordinating council of each participating sector.

“(II) Termination.—If the Director proceeds with the pilot described in ~~clause (ii)~~ *subclause (I)*, the pilot shall terminate on the date that is 2 years after the date on which the Director begins the pilot.

“(iii) Reports.—

“(I) Study.—Not later than 180 days after the date on which the Director completes the study conducted under clause (i), the Director shall submit to the appropriate congressional committees a report that—

“(aa) summarizes the study; and

“(bb) states whether the Director plans to proceed with the pilot described in clause (ii) *(I)*.

“(II) Pilot.—If the Director proceeds with the pilot described in clause (ii), not later than 1 year after the date on which the Director begins the pilot, the Director shall submit to the appropriate congressional committees a report that includes—

"(aa) a summary of the results of the pilot; and

"(bb) a recommendation as to whether the activities carried out under the pilot should be continued after the termination of the pilot described in clause (ii)(II).

"(3) COORDINATION WITH NATIONAL CYBER DIRECTOR.—The Director shall—

"(A) brief the National Cyber Director on the activities described in this subsection; and

"(B) coordinate activities with the National Cyber Director, as appropriate.

"(4) REPORTS.—

"(A) IN GENERAL.—Not later than 1 year after the date of enactment of this section, and every 2 years thereafter, the Director shall submit to the appropriate congressional committees a report that includes—

"(i) a summary of the work on open source software security performed by the Director during the period covered by the report, including a list of the Federal and non-Federal entities with which the Director interfaced;

"(ii) the framework developed under paragraph (2)(A);

"(iii) a summary of any updates made to the framework developed under paragraph (2)(A) pursuant to paragraph (2)(B) since the last report submitted under this subparagraph;

"(iv) a summary of ~~the~~ *each* assessment conducted pursuant to paragraph (2)(E) *since the last report was submitted under this subparagraph*;

"(v) a summary of changes made to the assessment conducted pursuant to paragraph (2)(E) since the last report submitted under this subparagraph, including overall security trends; and

"(vi) a summary of the types of entities with which ~~the~~ *an* assessment *conducted pursuant to paragraph (2)(E) since the last reported submitted under this subparagraph* was shared pursuant to paragraph (2)(H), including a list of the Federal and non-Federal entities with which the assessment was shared.

"(B) PUBLIC REPORT.—Not later than 30 days after the date on which the Director submits a report required under subparagraph (A), the Director shall make a version of the report publicly available on the website of the Agency.".

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by inserting after the item relating to section 2220E the following:

"Sec. 2220F. Open source software security duties.".

SEC. 4. SOFTWARE SECURITY ADVISORY SUBCOMMITTEE.

Section 2219(d)(1) of the Homeland Security Act of 2002 (6 U.S.C. 665e(d)(1)) is amended by adding at the end the following:

"(E) Software security, including open source software security.".

SEC. 5. OPEN SOURCE SOFTWARE GUIDANCE.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE CONGRESSIONAL COMMITTEE.—The term "appropriate congressional committee" has the meaning given the term in section

2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

(2) COVERED AGENCY.—The term ''covered agency'' means an agency described in section 901(b) of title 31, United States Code.

(3) DIRECTOR.—The term ''Director'' means the Director of the Office of Management and Budget.

(4) NATIONAL SECURITY SYSTEM.—The term ''national security system'' has the meaning given the term in section 3552 of title 44, United States Code.

(5) OPEN SOURCE SOFTWARE; OPEN SOURCE SOFTWARE COMMUNITY.—The terms ''open source software'' and ''open source software community'' have the meanings given those terms in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650), as amended by section 3 of this Act.

(b) GUIDANCE.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency, and the Administrator of General Services, shall issue guidance on the responsibilities

of the chief information officer at each covered agency regarding open source software, which shall include—

(A) how chief information officers at each covered agency should, considering industry and open source software community best practices—

(i) manage and reduce risks of using open source software; and

(ii) guide contributing to and releasing open source software;

(B) how chief information officers should enable, rather than inhibit, the secure usage of open source software at each covered agency;

(C) any relevant updates to the Memorandum M–16–21 issued by the Office of Management and Budget on August 8, 2016, entitled, ''Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software''; and

(D) how covered agencies may contribute publicly to open source software that the covered agency uses, including how chief information officers should encourage those contributions.

(2) EXEMPTION OF NATIONAL SECURITY SYSTEMS.—The guidance issued under paragraph (1) shall not apply to national security systems.

(c) PILOT.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the chief information officer of each covered agency selected under paragraph (2), in coordination with the Director, the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency, and the Administrator of General Services, shall establish a pilot open source function at the covered agency that—

(A) is modeled after open source program offices, such as those in the private sector, the nonprofit sector, academia, and other non-Federal entities; and

(B) shall—

(i) support the secure usage of open source software at the covered agency;

(ii) develop policies and processes for contributions to and releases of open source software at the covered agency, in consultation, as appropriate, with the offices of general counsel and procurement of the covered agency;

(iii) interface with the open source software community; and

(iv) manage and reduce risks of using open source software at the covered agency.

(2) SELECTION OF PILOT AGENCIES.—The Director, in coordination with the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency, and the Administrator of General Services, shall select not less than 1 and not more than 5 covered agencies to conduct the pilot described in paragraph (1).

(3) ASSESSMENT.—Not later than 1 year after the establishment of the pilot open source functions described in paragraph (1), the Director, in coordination with the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency, and the Administrator of General Services, shall assess whether open source functions should be established at some or all covered agencies, including—

(A) how to organize those functions within covered agencies, such as the creation of open source program offices; and

(B) appropriate roles and responsibilities for those functions.

(4) GUIDANCE.—Notwithstanding the termination of the pilot open source functions under paragraph (5), if the Director determines, based on the assessment described in paragraph (3), that some or all of the open source functions should be established at some or all covered agencies, the Director, in coordination with the National Cyber Director, the Director of the Cybersecurity and Infrastructure Security Agency, and the Administrator of General Services, shall issue guidance on the implementation of those functions.

(5) TERMINATION.—The pilot open source functions described in paragraph (1) shall terminate not later than 4 years after the establishment of the pilot open source functions.

(d) BRIEFING AND REPORT.—The Director shall—

(1) not later than 1 year after the date of enactment of this Act, brief the appropriate congressional committees on the guidance issued under subsection (b); and

(2) not later than 540 days after the establishment of the pilot open source functions under subsection (c)(1), submit to the appropriate congressional committees a report on—

(A) the pilot open source functions; and

(B) the results of the assessment conducted under subsection (c)(3).

(e) DUTIES.—Section 3554(b) of title 44, United States Code, is amended—

(1) in paragraph (7), by striking ‘‘and’’ at the end;

(2) in paragraph (8), by striking the period at the end and inserting ‘‘; and’’; and

(3) by adding at the end the following:

‘‘(9) plans and procedures to ensure the secure usage and development of software, including open source software *(as defined in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650))*.’’.

SEC. 6. RULE OF CONSTRUCTION.

Nothing in this Act or the amendments made by this Act shall be construed to provide any additional regulatory authority to any Federal agency described therein.

Calendar No. 76

118TH CONGRESS
1ST SESSION

S. 917

[Report No. 118–32]

A BILL

To establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software security, and for other purposes.

MAY 16, 2023

Reported with amendments