AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 3268

OFFERED BY MR. GREEN OF TENNESSEE

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

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

SEC. 2. 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 new paragraphs:

‘‘(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 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 such 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, and open source software communities; 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 one year after the date of the enactment of this section, the Director shall publicly publish a framework, incorporating government, private sector, 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, the following with respect to a given open source software component:

"(i) The security properties of code, such as whether the code is written in a memory-safe programming language or successor language.

"(ii) The security practices of development, build, and release processes, 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.

"(iv) The breadth of deployment.

"(v) The level of risk associated with where such component is integrated or deployed, such as whether such component operates on a network boundary or in a privileged location.

"(vi) The health and sustainability of the open source software community, including, where applicable, the level of current and historical investment and maintenance in such 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 such framework, including the augmentation, addition, or removal of the elements described in clauses (i) through (vi) of such subparagraph; and

“(ii) if the Director so determines that such additional updates are needed, make such updates.

“(C) DEVELOPING FRAMEWORK.—In developing the framework described in subparagraph (A), the Director shall consult with the following:

“(i) Appropriate Federal agencies, including the National Institute of Standards and Technology.

“(ii) 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 required under subparagraph (C).

"(E) FEDERAL OPEN SOURCE SOFTWARE ASSESSMENT.—Not later than one year after the publication of the framework under subparagraph (A) and not less frequently than every two years thereafter, the Director shall, to the greatest extent practicable and using such framework—

"(i) perform an assessment of each open source software component deployed on high value assets, as described in Office of Management and Budget memorandum M-19-03 (issued December 10, 2018) or successor guidance, at Federal agencies based on readily available, and, to the greatest extent practicable, machine readable, information, such as—

"(I) software bills of material 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, in consultation with the Federal agency at which an open source software component is deployed, one or more ranked lists of components described in clause (i) based on such 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 performed pursuant to subparagraph (E).

“(G) PUBLICATION.—The Director shall publicly publish and maintain any tools developed to perform the assessment under subparagraph (E) as open source software.

"(H) SHARING.—

"(i) RESULTS.—The Director, to the greatest extent practicable, and taking into account the sensitivity of the information contained in the assessment performed pursuant to subparagraph (E), shall facilitate the sharing of the results of each assessment under 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 an assessment under subparagraph (E)(i).

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

"(i) STUDY.—Not later than two years after the publication of the framework under subparagraph (A), the Director shall conduct a study regarding the feasibility of the Director conducting the assessment under 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 one 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 assessment described in subclause (I), such pilot assessment shall terminate not later than two years after the date on which the Director begins such pilot assessment.

"(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;

''(bb) states whether the Director plans to proceed with the pilot assessment described in clause (ii)(I); and

''(cc) if the Director proceeds with such pilot assessment, describes—

''(AA) the methodology for selecting the critical infrastructure sector or sectors to participate in the pilot; and

''(BB) the resources required to carry out the pilot.

''(II) PILOT.—If the Director proceeds with the pilot assessment described in clause (ii), not later than one year after the date on which the

Director begins such pilot assessment, the Director shall submit to the appropriate congressional committees a report that includes the following:

"(aa) A summary of the results of such pilot assessment.

"(bb) A recommendation as to whether the activities carried out under such pilot assessment should be continued after the termination of such pilot assessment in accordance with clause (ii)(II).

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

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

"(B) consult with the National Cyber Director regarding such activities, as appropriate.

"(4) REPORTS.—

"(A) IN GENERAL.—Not later than one year after the date of the enactment of this section and every two years thereafter for the following six years, the Director shall submit to the appropriate congressional committees a report that includes for the period covered by each such report the following:

“(i) A summary of the work on open source software security performed by the Director, including a list of the Federal and non-Federal entities with which the Director interfaced.

“(ii) The framework under paragraph (2)(A) or a summary of any updates to such framework pursuant to paragraph (2)(B), as the case may be.

“(iii) A summary of each assessment under paragraph (2)(E)(i).

“(iv) A summary of changes made to each such assessment, including overall security trends.

“(v) A summary of the types of entities with which each such assessment was shared pursuant to paragraph (2)(H), including a list of the Federal and non-Federal entities with which such assessment was shared.

“(vi) Information on resources, including staffing, allocated to the Director’s open source software responsibilities under this section.

“(B) PUBLIC REPORT.—Not later than 30 days after the date on which the Director submits each report required under subparagraph (A), the Director shall make a version of each such 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 is amended by inserting after the item relating to section 2220E the following new item:

“Sec. 2220F. Open source software security duties.”.

(c) 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.”.

(d) RULE OF CONSTRUCTION.—Nothing in this Act or the amendments made by this Act may be construed to provide any additional regulatory authority to any Federal agency described therein.