

.....  
(Original Signature of Member)

118TH CONGRESS  
1ST SESSION

# H. R. 3286

To amend the Homeland Security Act of 2002 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 HOUSE OF REPRESENTATIVES

Mr. GREEN of Tennessee introduced the following bill; which was referred to the Committee on \_\_\_\_\_

---

## A BILL

To amend the Homeland Security Act of 2002 to establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software security, 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 “Securing Open Source  
5 Software Act of 2023”.

1 **SEC. 2. OPEN SOURCE SOFTWARE SECURITY DUTIES.**

2 (a) IN GENERAL.—Title XXII of the Homeland Se-  
3 curity Act of 2002 (6 U.S.C. 650 et seq.) is amended—

4 (1) in section 2200 (6 U.S.C. 650)—

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

8 (B) by inserting after paragraph (21) the  
9 following new paragraphs:

10 “(22) OPEN SOURCE SOFTWARE.—The term  
11 ‘open source software’ means software for which the  
12 human-readable source code is made available to the  
13 public for use, study, re-use, modification, enhance-  
14 ment, and re-distribution.

15 “(23) OPEN SOURCE SOFTWARE COMMUNITY.—  
16 The term ‘open source software community’ means  
17 the community of individuals, foundations, nonprofit  
18 organizations, corporations, and other entities  
19 that—

20 “(A) develop, contribute to, maintain, and  
21 publish open source software; or

22 “(B) otherwise work to ensure the security  
23 of the open source software ecosystem.

24 “(24) OPEN SOURCE SOFTWARE COMPONENT.—  
25 The term ‘open source software component’ means

1 an individual repository of open source software that  
2 is made available to the public.”;

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

4 (A) in paragraph (13), by striking “and”  
5 at the end;

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

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

10 “(14) support, including by offering services,  
11 the secure usage and deployment of software, includ-  
12 ing open source software, in the software develop-  
13 ment lifecycle at Federal agencies in accordance with  
14 section 2220F; and”;

15 (3) by adding at the end the following:

16 **“SEC. 2220F. OPEN SOURCE SOFTWARE SECURITY DUTIES.**

17 “(a) DEFINITION.—In this section, the term ‘soft-  
18 ware bill of materials’ has the meaning given such term  
19 in the Minimum Elements for a Software Bill of Materials  
20 published by the Department of Commerce, or any super-  
21 seding definition published by the Agency.

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

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

3           “(2) perform the duties described in subsection  
4           (c).

5           “(c) DUTIES OF THE DIRECTOR.—

6           “(1) IN GENERAL.—The Director shall—

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

9                   “(B) support Federal efforts to strengthen  
10                  the security of open source software;

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

14                  “(D) serve as a public point of contact re-  
15                  garding the security of open source software for  
16                  non-Federal entities, including State, local,  
17                  Tribal, and territorial partners, the private sec-  
18                  tor, international partners, and open source  
19                  software communities; and

20                  “(E) support Federal and non-Federal  
21                  supply chain security efforts by encouraging ef-  
22                  forts to bolster open source software security,  
23                  such as—

24                          “(i) assisting in coordinated vulner-  
25                          ability disclosures in open source software

1 components pursuant to section 2209(n);  
2 and

3 “(ii) supporting the activities of the  
4 Federal Acquisition Security Council.

5 “(2) ASSESSMENT OF CRITICAL OPEN SOURCE  
6 SOFTWARE COMPONENTS.—

7 “(A) FRAMEWORK.—Not later than one  
8 year after the date of the enactment of this sec-  
9 tion, the Director shall publicly publish a  
10 framework, incorporating government, private  
11 sector, and open source software community  
12 frameworks and best practices, including those  
13 published by the National Institute of Stand-  
14 ards and Technology, for assessing the risk of  
15 open source software components, including di-  
16 rect and indirect open source software depend-  
17 encies, which shall incorporate, at a minimum,  
18 the following with respect to a given open  
19 source software component:

20 “(i) The security properties of code,  
21 such as whether the code is written in a  
22 memory-safe programming language.

23 “(ii) The security practices of develop-  
24 ment, build, and release processes, such as  
25 the use of multi-factor authentication by

1 maintainers and cryptographic signing of  
2 releases.

3 “(iii) The number and severity of pub-  
4 licly known, unpatched vulnerabilities.

5 “(iv) The breadth of deployment.

6 “(v) The level of risk associated with  
7 where such component is integrated or de-  
8 ployed, such as whether such component  
9 operates on a network boundary or in a  
10 privileged location.

11 “(vi) The health of the open source  
12 software community, including, where ap-  
13 plicable, the level of current and historical  
14 investment and maintenance in such com-  
15 ponent, such as the number and activity of  
16 individual maintainers.

17 “(B) UPDATING FRAMEWORK.—Not less  
18 frequently than annually after the date on  
19 which the framework is published under sub-  
20 paragraph (A), the Director shall—

21 “(i) determine whether updates are  
22 needed to such framework, including the  
23 augmentation, addition, or removal of the  
24 elements described in clauses (i) through  
25 (vi) of such subparagraph; and

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

4                   “(C) DEVELOPING FRAMEWORK.—In de-  
5                   veloping the framework described in subpara-  
6                   graph (A), the Director shall consult with the  
7                   following:

8                   “(i) Appropriate Federal agencies, in-  
9                   cluding the National Institute of Standards  
10                  and Technology.

11                  “(ii) Individuals and nonprofit organi-  
12                  zations from the open source software com-  
13                  munity.

14                  “(iii) Private sector entities from the  
15                  open source software community.

16                  “(D) USABILITY.—The Director shall en-  
17                  sure, to the greatest extent practicable, that the  
18                  framework described in subparagraph (A) is us-  
19                  able by the open source software community,  
20                  including through the consultation required  
21                  under subparagraph (C).

22                  “(E) FEDERAL OPEN SOURCE SOFTWARE  
23                  ASSESSMENT.—Not later than one year after  
24                  the publication of the framework under sub-  
25                  paragraph (A) and not less frequently than

1 every two years thereafter, the Director shall, to  
2 the greatest extent practicable and using such  
3 framework—

4 “(i) perform an assessment of each  
5 open source software component used di-  
6 rectly or indirectly by Federal agencies  
7 based on readily available, and, to the  
8 greatest extent practicable, machine read-  
9 able, information, such as—

10 “(I) software bills of material  
11 that are, at the time of the assess-  
12 ment, made available to the Agency or  
13 are otherwise accessible via the inter-  
14 net;

15 “(II) software inventories, avail-  
16 able to the Director at the time of the  
17 assessment, from the Continuous  
18 Diagnostics and Mitigation program  
19 of the Agency; and

20 “(III) other publicly available in-  
21 formation regarding open source soft-  
22 ware components; and

23 “(ii) develop one or more ranked lists  
24 of components described in clause (i) based  
25 on the assessment, such as ranked by the



1           criticality, level of risk, or usage of the  
2           components, or a combination thereof.

3           “(F) AUTOMATION.—The Director shall, to  
4           the greatest extent practicable, automate the  
5           assessment performed pursuant to subpara-  
6           graph (E).

7           “(G) PUBLICATION.—The Director shall  
8           publicly publish and maintain any tools devel-  
9           oped to perform the assessment under subpara-  
10          graph (E) as open source software.

11          “(H) SHARING.—

12           “(i) RESULTS.—The Director shall fa-  
13           cilitate the sharing of the results of each  
14           assessment under subparagraph (E)(i)  
15           with appropriate Federal and non-Federal  
16           entities working to support the security of  
17           open source software, including by offering  
18           means for appropriate Federal and non-  
19           Federal entities to download the assess-  
20           ment in an automated manner.

21           “(ii) DATASETS.—The Director may  
22           publicly publish, as appropriate, any  
23           datasets or versions of the datasets devel-  
24           oped or consolidated as a result of an as-  
25           sessment under subparagraph (E)(i).

1                   “(I) CRITICAL INFRASTRUCTURE ASSESS-  
2                   MENT STUDY AND PILOT.—

3                   “(i) STUDY.—Not later than two  
4                   years after the publication of the frame-  
5                   work under subparagraph (A), the Director  
6                   shall conduct a study regarding the feasi-  
7                   bility of the Director conducting the as-  
8                   sessment under subparagraph (E) for crit-  
9                   ical infrastructure entities.

10                   “(ii) PILOT.—

11                   “(I) IN GENERAL.—If the Direc-  
12                   tor determines that the assessment  
13                   described in clause (i) is feasible, the  
14                   Director may conduct a pilot assess-  
15                   ment on a voluntary basis with one or  
16                   more critical infrastructure sectors, in  
17                   coordination with the Sector Risk  
18                   Management Agency and the sector  
19                   coordinating council of each partici-  
20                   pating sector.

21                   “(II) TERMINATION.—If the Di-  
22                   rector proceeds with the pilot assess-  
23                   ment described in subclause (I), such  
24                   pilot assessment shall terminate not  
25                   later than two years after the date on

1 which the Director begins such pilot  
2 assessment.

3 “(iii) REPORTS.—

4 “(I) STUDY.—Not later than 180  
5 days after the date on which the Di-  
6 rector completes the study conducted  
7 under clause (i), the Director shall  
8 submit to the appropriate congress-  
9 sional committees a report that—

10 “(aa) summarizes the study;

11 and

12 “(bb) states whether the Di-  
13 rector plans to proceed with the  
14 pilot assessment described in  
15 clause (ii)(I).

16 “(II) PILOT.—If the Director  
17 proceeds with the pilot assessment de-  
18 scribed in clause (ii), not later than  
19 one year after the date on which the  
20 Director begins such pilot assessment,  
21 the Director shall submit to the ap-  
22 propriate congressional committees a  
23 report that includes the following:

24 “(aa) A summary of the re-  
25 sults of such pilot assessment.

1                   “(bb) A recommendation as  
2                   to whether the activities carried  
3                   out under such pilot assessment  
4                   should be continued after the ter-  
5                   mination of such pilot assessment  
6                   in accordance with clause (ii)(II).

7                   “(3) COORDINATION WITH NATIONAL CYBER DI-  
8                   RECTOR.—The Director shall—

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

11                  “(B) consult with the National Cyber Di-  
12                  rector regarding such activities, as appropriate.

13                  “(4) REPORTS.—

14                  “(A) IN GENERAL.—Not later than one  
15                  year after the date of the enactment of this sec-  
16                  tion and every two years thereafter, the Direc-  
17                  tor shall submit to the appropriate congres-  
18                  sional committees a report that includes for the  
19                  period covered by each such report the fol-  
20                  lowing:

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

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

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

7 “(iv) A summary of changes made to  
8 each such assessment, including overall se-  
9 curity trends.

10 “(v) A summary of the types of enti-  
11 ties with which each such assessment was  
12 shared pursuant to paragraph (2)(H), in-  
13 cluding a list of the Federal and non-Fed-  
14 eral entities with which such assessment  
15 was shared.

16 “(B) PUBLIC REPORT.—Not later than 30  
17 days after the date on which the Director sub-  
18 mits each report required under subparagraph  
19 (A), the Director shall make a version of each  
20 such report publicly available on the website of  
21 the Agency.”.

22 (b) TECHNICAL AND CONFORMING AMENDMENT.—  
23 The table of contents in section 1(b) of the Homeland Se-  
24 curity Act of 2002 is amended by inserting after the item  
25 relating to section 2220E the following new item:

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

1           (c) SOFTWARE SECURITY ADVISORY SUB-  
2 COMMITTEE.—Section 2219(d)(1) of the Homeland Secu-  
3 rity Act of 2002 (6 U.S.C. 665e(d)(1)) is amended by add-  
4 ing at the end the following:

5                       “(E) Software security, including open  
6                       source software security.”.

7           (d) RULE OF CONSTRUCTION.—Nothing in this Act  
8 or the amendments made by this Act may be construed  
9 to provide any additional regulatory authority to any Fed-  
10 eral agency described therein.