

118TH CONGRESS
1ST SESSION

S. _____

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

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

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.

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”.

6 **SEC. 2. FINDINGS.**

7 Congress finds that—

1 (1) open source software fosters technology de-
2 velopment and is an integral part of overall cyberse-
3 curity;

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

8 (3) open source software is part of the founda-
9 tion of digital infrastructure that promotes a free
10 and open internet;

11 (4) due to both the unique strengths of open
12 source software and inconsistent historical invest-
13 ment in open source software security, there exist
14 unique challenges in securing open source software;
15 and

16 (5) the Federal Government should play a sup-
17 porting role in ensuring the long-term security of
18 open source software.

19 **SEC. 3. OPEN SOURCE SOFTWARE SECURITY DUTIES.**

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

22 (1) in section 2200 (6 U.S.C. 650)—

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

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

3 “(22) OPEN SOURCE SOFTWARE.—The term
4 ‘open source software’ means software for which the
5 human-readable source code is made available to the
6 public for use, study, re-use, modification, enhance-
7 ment, and re-distribution.

8 “(23) OPEN SOURCE SOFTWARE COMMUNITY.—
9 The term ‘open source software community’ means
10 the community of individuals, foundations, nonprofit
11 organizations, corporations, and other entities
12 that—

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

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

17 “(24) OPEN SOURCE SOFTWARE COMPONENT.—
18 The term ‘open source software component’ means
19 an individual repository of open source software that
20 is made available to the public.”;

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

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

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

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

3 “(14) support, including by offering services,
4 the secure usage and deployment of software, includ-
5 ing open source software, in the software develop-
6 ment lifecycle at Federal agencies in accordance with
7 section 2220E; and”;

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

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

10 “(a) DEFINITION.—In this section, the term ‘soft-
11 ware bill of materials’ has the meaning given the term in
12 the Minimum Elements for a Software Bill of Materials
13 published by the Department of Commerce, or any super-
14 seding definition published by the Agency.

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

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

20 “(2) perform the duties described in subsection
21 (c).

22 “(c) DUTIES OF THE DIRECTOR.—

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

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

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

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

6 “(D) serve as a public point of contact re-
7 garding the security of open source software for
8 non-Federal entities, including State, local,
9 Tribal, and territorial partners, the private sec-
10 tor, international partners, open source soft-
11 ware organizations, and open source software
12 developers; and

13 “(E) support Federal and non-Federal
14 supply chain security efforts by encouraging ef-
15 forts to bolster open source software security,
16 such as—

17 “(i) assisting in coordinated vulner-
18 ability disclosures in open source software
19 components pursuant to section 2209(n);
20 and

21 “(ii) supporting the activities of the
22 Federal Acquisition Security Council.

23 “(2) ASSESSMENT OF CRITICAL OPEN SOURCE
24 SOFTWARE COMPONENTS.—

1 “(A) FRAMEWORK.—Not later than 1 year
2 after the date of enactment of this section, the
3 Director shall publicly publish a framework, in-
4 corporating government, industry, and open
5 source software community frameworks and
6 best practices, including those published by the
7 National Institute of Standards and Tech-
8 nology, for assessing the risk of open source
9 software components, including direct and indi-
10 rect open source software dependencies, which
11 shall incorporate, at a minimum—

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

16 “(ii) the security practices of develop-
17 ment, build, and release processes of a
18 given open source software component,
19 such as the use of multi-factor authentica-
20 tion by maintainers and cryptographic
21 signing of releases;

22 “(iii) the number and severity of pub-
23 licly known, unpatched vulnerabilities in a
24 given open source software component;

1 “(iv) the breadth of deployment of a
2 given open source software component;

3 “(v) the level of risk associated with
4 where a given open source software compo-
5 nent is integrated or deployed, such as
6 whether the component operates on a net-
7 work boundary or in a privileged location;
8 and

9 “(vi) the health of the community for
10 a given open source software component,
11 including, where applicable, the level of
12 current and historical investment and
13 maintenance in the open source software
14 component, such as the number and activ-
15 ity of individual maintainers.

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

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

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

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

7 “(i) appropriate Federal agencies, in-
8 cluding the National Institute of Standards
9 and Technology;

10 “(ii) individuals and nonprofit organi-
11 zations from the open source software com-
12 munity; and

13 “(iii) private companies from the open
14 source software community.

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

21 “(E) FEDERAL OPEN SOURCE SOFTWARE
22 ASSESSMENT.—Not later than 1 year after the
23 publication of the framework described in sub-
24 paragraph (A), and not less frequently than
25 every 2 years thereafter, the Director shall, to

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

3 “(i) STUDY.—Not later than 2 years
4 after the publication of the framework de-
5 scribed in subparagraph (A), the Director
6 shall conduct a study regarding the feasi-
7 bility of the Director conducting the as-
8 sessment described in subparagraph (E)
9 for critical 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 1 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 de-
23 scribed in clause (ii), the pilot shall
24 terminate on the date that is 2 years

1 after the date on which the Director
2 begins the pilot.

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 described in clause (ii).

15 “(II) PILOT.—If the Director
16 proceeds with the pilot described in
17 clause (ii), not later than 1 year after
18 the date on which the Director begins
19 the pilot, the Director shall submit to
20 the appropriate congressional commit-
21 tees a report that includes—

22 “(aa) a summary of the re-
23 sults of the pilot; and

24 “(bb) a recommendation as
25 to whether the activities carried

1 out under the pilot should be
2 continued after the termination
3 of the pilot described in clause
4 (ii)(II).

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

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

9 “(B) coordinate activities with the Na-
10 tional Cyber Director, as appropriate.

11 “(4) REPORTS.—

12 “(A) IN GENERAL.—Not later than 1 year
13 after the date of enactment of this section, and
14 every 2 years thereafter, the Director shall sub-
15 mit to the appropriate congressional committees
16 a report that includes—

17 “(i) a summary of the work on open
18 source software security performed by the
19 Director during the period covered by the
20 report, including a list of the Federal and
21 non-Federal entities with which the Direc-
22 tor interfaced;

23 “(ii) the framework developed under
24 paragraph (2)(A);

1 “(iii) a summary of any updates made
2 to the framework developed under para-
3 graph (2)(A) pursuant to paragraph
4 (2)(B) since the last report submitted
5 under this subparagraph;

6 “(iv) a summary of the assessment
7 conducted pursuant to paragraph (2)(E);

8 “(v) a summary of changes made to
9 the assessment conducted pursuant to
10 paragraph (2)(E) since the last report sub-
11 mitted under this subparagraph, including
12 overall security trends; and

13 “(vi) a summary of the types of enti-
14 ties with which the assessment was shared
15 pursuant to paragraph (2)(H), including a
16 list of the Federal and non-Federal entities
17 with which the assessment was shared.

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

24 (b) TECHNICAL AND CONFORMING AMENDMENT.—
25 The table of contents in section 1(b) of the Homeland Se-

1 security Act of 2002 (Public Law 107–296; 116 Stat. 2135)
2 is amended by inserting after the item relating to section
3 2220E the following:

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

4 **SEC. 4. SOFTWARE SECURITY ADVISORY SUBCOMMITTEE.**

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

8 “(E) Software security, including open
9 source software security.”.

10 **SEC. 5. OPEN SOURCE SOFTWARE GUIDANCE.**

11 (a) DEFINITIONS.—In this section:

12 (1) APPROPRIATE CONGRESSIONAL COM-
13 MITTEE.—The term “appropriate congressional com-
14 mittee” has the meaning given the term in section
15 2 of the Homeland Security Act of 2002 (6 U.S.C.
16 101).

17 (2) COVERED AGENCY.—The term “covered
18 agency” means an agency described in section
19 901(b) of title 31, United States Code.

20 (3) DIRECTOR.—The term “Director” means
21 the Director of the Office of Management and Budg-
22 et.

23 (4) NATIONAL SECURITY SYSTEM.—The term
24 “national security system” has the meaning given

1 the term in section 3552 of title 44, United States
2 Code.

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

9 (b) GUIDANCE.—

10 (1) IN GENERAL.—Not later than 1 year after
11 the date of enactment of this Act, the Director, in
12 coordination with the National Cyber Director, the
13 Director of the Cybersecurity and Infrastructure Se-
14 curity Agency, and the Administrator of General
15 Services, shall issue guidance on the responsibilities
16 of the chief information officer at each covered agen-
17 cy regarding open source software, which shall in-
18 clude—

19 (A) how chief information officers at each
20 covered agency should, considering industry and
21 open source software community best prac-
22 tices—

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

1 (ii) guide contributing to and releas-
2 ing open source software;

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

6 (C) any relevant updates to the Memo-
7 randum M-16-21 issued by the Office of Man-
8 agement and Budget on August 8, 2016, enti-
9 tled, “Federal Source Code Policy: Achieving
10 Efficiency, Transparency, and Innovation
11 through Reusable and Open Source Software”;
12 and

13 (D) how covered agencies may contribute
14 publicly to open source software that the cov-
15 ered agency uses, including how chief informa-
16 tion officers should encourage those contribu-
17 tions.

18 (2) EXEMPTION OF NATIONAL SECURITY SYS-
19 TEMS.—The guidance issued under paragraph (1)
20 shall not apply to national security systems.

21 (c) PILOT.—

22 (1) IN GENERAL.—Not later than 1 year after
23 the date of enactment of this Act, the chief informa-
24 tion officer of each covered agency selected under
25 paragraph (2), in coordination with the Director, the

1 National Cyber Director, the Director of the Cyber-
2 security and Infrastructure Security Agency, and the
3 Administrator of General Services, shall establish a
4 pilot open source function at the covered agency
5 that—

6 (A) is modeled after open source program
7 offices, such as those in the private sector, the
8 nonprofit sector, academia, and other non-Fed-
9 eral entities; and

10 (B) shall—

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

13 (ii) develop policies and processes for
14 contributions to and releases of open
15 source software at the covered agency, in
16 consultation, as appropriate, with the of-
17 fices of general counsel and procurement of
18 the covered agency;

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

21 (iv) manage and reduce risks of using
22 open source software at the covered agen-
23 cy.

24 (2) SELECTION OF PILOT AGENCIES.—The Di-
25 rector, in coordination with the National Cyber Di-

1 rector, the Director of the Cybersecurity and Infra-
2 structure Security Agency, and the Administrator of
3 General Services, shall select not less than 1 and not
4 more than 5 covered agencies to conduct the pilot
5 described in paragraph (1).

6 (3) ASSESSMENT.—Not later than 1 year after
7 the establishment of the pilot open source functions
8 described in paragraph (1), the Director, in coordi-
9 nation with the National Cyber Director, the Direc-
10 tor of the Cybersecurity and Infrastructure Security
11 Agency, and the Administrator of General Services,
12 shall assess whether open source functions should be
13 established at some or all covered agencies, includ-
14 ing—

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

18 (B) appropriate roles and responsibilities
19 for those functions.

20 (4) GUIDANCE.—Notwithstanding the termi-
21 nation of the pilot open source functions under para-
22 graph (5), if the Director determines, based on the
23 assessment described in paragraph (3), that some or
24 all of the open source functions should be estab-
25 lished at some or all covered agencies, the Director,

1 in coordination with the National Cyber Director,
2 the Director of the Cybersecurity and Infrastructure
3 Security Agency, and the Administrator of General
4 Services, shall issue guidance on the implementation
5 of those functions.

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

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

11 (1) not later than 1 year after the date of en-
12 actment of this Act, brief the appropriate congres-
13 sional committees on the guidance issued under sub-
14 section (b); and

15 (2) not later than 540 days after the establish-
16 ment of the pilot open source functions under sub-
17 section (c)(1), submit to the appropriate congres-
18 sional committees a report on—

19 (A) the pilot open source functions; and

20 (B) the results of the assessment con-
21 ducted under subsection (c)(3).

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

24 (1) in paragraph (7), by striking “and” at the
25 end;

1 (2) in paragraph (8), by striking the period at
2 the end and inserting “; and”; and

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

4 “(9) plans and procedures to ensure the secure
5 usage and development of software, including open
6 source software.”.

7 **SEC. 6. RULE OF CONSTRUCTION.**

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