

117TH CONGRESS  
2D SESSION

# S. 4913

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

SEPTEMBER 21, 2022

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

---

## 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 2022”.

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.—Subtitle A of title XXII of the  
21          Homeland Security Act of 2002 (6 U.S.C. 651 et seq.)  
22          is amended—

23                 (1) in section 2201 (6 U.S.C. 651)—

1 (A) by redesignating paragraphs (5), (6),  
2 and (7) as paragraphs (8), (9), and (10), re-  
3 spectively; and

4 (B) by inserting after paragraph (4) the  
5 following:

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

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

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

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

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

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

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

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

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

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

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

13 **“SEC. 2220E. OPEN SOURCE SOFTWARE SECURITY DUTIES.**

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

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

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

24 “(2) perform the duties described in subsection  
25 (c).

1 “(c) DUTIES OF THE DIRECTOR.—

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

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

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

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

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

17 “(E) support Federal and non-Federal  
18 supply chain security efforts by encouraging ef-  
19 forts to bolster open source security, such as—

20 “(i) assisting in coordinated vulner-  
21 ability disclosures in open source software  
22 components pursuant to section 2209(n);  
23 and

24 “(ii) supporting the activities of the  
25 Federal Acquisition Security Council.

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

3           “(A) FRAMEWORK.—Not later than 1 year  
4 after the date of enactment of this section, the  
5 Director shall publicly publish a framework, in-  
6 corporating government, including those pub-  
7 lished by the National Institute of Standards  
8 and Technology, industry, and open source soft-  
9 ware community frameworks and best practices,  
10 for assessing the risk of open source software  
11 components, including direct and indirect open  
12 source software dependencies, which shall incor-  
13 porate, at a minimum—

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

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

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

4           “(iv) the breadth of deployment of a  
5           given open source software component;

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

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

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

23                 “(i) determine whether additional up-  
24                 dates are needed to the framework de-  
25                 scribed in subparagraph (A); 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) FEDERAL OPEN SOURCE SOFTWARE  
16           ASSESSMENT.—Not later than 1 year after the  
17           publication of the framework described in sub-  
18           paragraph (A), and not less frequently than  
19           every 2 years thereafter, the Director shall, to  
20           the greatest extent practicable and using the  
21           framework described in subparagraph (A)—

22                   “(i) perform an assessment of open  
23                   source software components used directly  
24                   or indirectly by Federal agencies based on  
25                   readily available, and, to the greatest ex-



1           tent practicable, machine readable, infor-  
2           mation, such as—

3                   “(I) software bills of material  
4                   that are made available to the Agency  
5                   or are otherwise accessible via the  
6                   internet;

7                   “(II) software inventories col-  
8                   lected from the Continuous  
9                   Diagnostics and Mitigation program  
10                  of the Agency; and

11                  “(III) other publicly available in-  
12                  formation regarding open source soft-  
13                  ware components; and

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

19                  “(E) AUTOMATION.—The Director shall,  
20                  to the greatest extent practicable, automate the  
21                  assessment conducted under subparagraph (D).

22                  “(F) PUBLICATION.—The Director shall  
23                  publicly publish and maintain any tools devel-  
24                  oped to conduct the assessment described in  
25                  subparagraph (D) as open source software.

1 “(G) SHARING.—

2 “(i) RESULTS.—The Director shall fa-  
3 cilitate the sharing of the results of the as-  
4 sessment described in subparagraph (D)  
5 with appropriate Federal and non-Federal  
6 entities working to support the security of  
7 open source software, including by offering  
8 means for appropriate Federal and non-  
9 Federal entities to download the assess-  
10 ment in an automated manner.

11 “(ii) DATASETS.—The Director may  
12 publicly publish, as appropriate, any  
13 datasets or versions of the datasets devel-  
14 oped or consolidated as a result of the as-  
15 sessment described in subparagraph (D).

16 “(H) CRITICAL INFRASTRUCTURE ASSESS-  
17 MENT STUDY AND PILOT.—

18 “(i) STUDY.—Not later than 2 years  
19 after the publication of the framework de-  
20 scribed in subparagraph (A), the Director  
21 shall conduct a study regarding the feasi-  
22 bility of the Director conducting the as-  
23 sessment described in subparagraph (D)  
24 for critical infrastructure entities.

1           “(ii) PILOT.—If the Director deter-  
2 mines that the assessment described in  
3 clause (i) is feasible, the Director may con-  
4 duct a pilot assessment on a voluntary  
5 basis with 1 or more critical infrastructure  
6 sectors, in coordination with the Sector  
7 Risk Management Agency and the sector  
8 coordinating council of each participating  
9 sector.

10           “(iii) REPORTS.—

11           “(I) STUDY.—Not later than 180  
12 days after the date on which the Di-  
13 rector completes the study conducted  
14 under clause (i), the Director shall  
15 submit to the appropriate congress-  
16 sional committees a report that—

17           “(aa) summarizes the study;

18           and

19           “(bb) states whether the Di-  
20 rector plans to proceed with the  
21 pilot described in clause (ii).

22           “(II) PILOT.—If the Director  
23 proceeds with the pilot described in  
24 clause (ii), not later than 1 year after  
25 the date on which the Director begins

1 the pilot, the Director shall submit to  
2 the appropriate congressional commit-  
3 tees a report that includes—

4 “(aa) a summary of the re-  
5 sults of the pilot; and

6 “(bb) a recommendation as  
7 to whether the pilot should be  
8 continued.

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

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

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

15 “(4) REPORTS.—

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

21 “(i) a summary of the work on open  
22 source software security performed by the  
23 Director during the period covered by the  
24 report, including a list of the Federal and

1 non-Federal entities with which the Direc-  
2 tor interfaced;

3 “(ii) the framework developed under  
4 paragraph (2)(A);

5 “(iii) a summary of changes made to  
6 the framework developed under paragraph  
7 (2)(A) since the last report submitted  
8 under this subparagraph;

9 “(iv) a summary of the assessment  
10 conducted pursuant to paragraph (2)(D);

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

16 “(vi) a summary of the types of enti-  
17 ties with which the assessment was shared  
18 pursuant to paragraph (2)(G), including a  
19 list of the Federal and non-Federal entities  
20 with which the assessment was shared.

21 “(B) PUBLIC REPORT.—Not later than 30  
22 days after the date on which the Director sub-  
23 mits a report required under subparagraph (A),  
24 the Director shall make a version of the report

1 publicly available on the website of the Agen-  
2 cy.”.

3 (b) TECHNICAL AND CONFORMING AMENDMENT.—

4 The table of contents in section 1(b) of the Homeland Se-  
5 curity Act of 2002 (Public Law 107–296; 116 Stat. 2135)  
6 is amended—

7 (1) by moving the item relating to section  
8 2220D to appear after the item relating to section  
9 2220C; and

10 (2) by inserting after the item relating to sec-  
11 tion 2220D the following:

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

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

13 Section 2219(d)(1) of the Homeland Security Act of  
14 2002 (6 U.S.C. 665e(d)(1)) is amended by adding at the  
15 end the following:

16 “(E) Software security, including open  
17 source software security.”.

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

19 (a) DEFINITIONS.—In this section:

20 (1) APPROPRIATE CONGRESSIONAL COM-  
21 MITTEE.—The term “appropriate congressional com-  
22 mittee” has the meaning given the term in section  
23 2 of the Homeland Security Act of 2002 (6 U.S.C.  
24 101).

1           (2) COVERED AGENCY.—The term “covered  
2 agency” means an agency described in section  
3 901(b) of title 31, United States Code.

4           (3) DIRECTOR.—The term “Director” means  
5 the Director of the Office of Management and Budg-  
6 et.

7           (4) OPEN SOURCE SOFTWARE; OPEN SOURCE  
8 SOFTWARE COMMUNITY.—The terms “open source  
9 software” and “open source software community”  
10 have the meanings given those terms in section 2201  
11 of the Homeland Security Act of 2002 (6 U.S.C.  
12 651), as amended by section 3 of this Act.

13       (b) GUIDANCE.—

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

23                   (A) how chief information officers at each  
24 covered agency should, considering industry and

1 open source software community best prac-  
2 tices—

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

5 (ii) guide contributing to and releas-  
6 ing open source software;

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

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

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

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

25 (c) PILOT.—



1           (1) IN GENERAL.—Not later than 1 year after  
2 the date of enactment of this Act, the chief informa-  
3 tion officer of each covered agency described in para-  
4 graph (2), in coordination with the Director, the Na-  
5 tional Cyber Director, the Director of the Cybersecu-  
6 rity and Infrastructure Security Agency, and the  
7 Administrator of General Services, shall establish a  
8 pilot open source function at the covered agency  
9 that—

10           (A) is modeled after open source program  
11 offices, such as those in the private sector, the  
12 nonprofit sector, academia, and other non-Fed-  
13 eral entities; and

14           (B) shall—

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

17           (ii) develop policies and processes for  
18 contributions to and releases of open  
19 source software at the covered agency, in  
20 consultation, as appropriate, with the Of-  
21 fices of General Counsel and Procurement  
22 of the covered agency;

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

1 (iv) manage and reduce risks of con-  
2 suming open source software at the cov-  
3 ered agency.

4 (2) SELECTION OF PILOT AGENCIES.—The Di-  
5 rector, in coordination with the National Cyber Di-  
6 rector, the Director of the Cybersecurity and Infra-  
7 structure Security Agency, and the Administrator of  
8 General Services, shall select 1 or more covered  
9 agencies to conduct the pilot described in paragraph  
10 (1)

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

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

23 (B) appropriate roles and responsibilities  
24 for those functions.

1           (4) GUIDANCE.—If the Director determines,  
2           based on the assessment described in paragraph (3),  
3           that some or all of the open source functions should  
4           be established at some or all covered agencies, the  
5           Director, in coordination with the National Cyber  
6           Director, the Director of the Cybersecurity and In-  
7           frastructure Security Agency, and the Administrator  
8           of General Services, shall issue guidance on the im-  
9           plementation of those 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.

○