Calendar No. 76

118TH CONGRESS *1st Session*	SENATE	REPORT 118–32

SECURING OPEN SOURCE SOFTWARE ACT OF 2023

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 917

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.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
39–010 WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	RAND PAUL, Kentucky
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	JAMES LANKFORD, Oklahoma
JACKY ROSEN, Nevada	MITT ROMNEY, Utah
ALEX PADILLA, California	RICK SCOTT, Florida
JON OSSOFF, Georgia	JOSH HAWLEY, Missouri
RICHARD BLUMENTHAL, Connecticut	ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*
WILLIAM E. HENDERSON III, *Minority Staff Director*
CHRISTINA N. SALAZAR, *Minority Chief Counsel*
KENDAL B. TIGNER, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 76

118TH CONGRESS *1st Session* | SENATE | REPORT 118–32

SECURING OPEN SOURCE SOFTWARE ACT OF 2023

MAY 16, 2023.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 917]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 917) to establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software security, and for other purposes, having considered the same, reports favorably thereon with amendments and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 917, the *Securing Open Source Software Act of 2023*, would authorize a number of activities at the Cybersecurity and Infrastructure Security Agency (CISA) to support the security of open source software in the Federal government and in private sector critical infrastructure. The bill would require CISA to publish and use a framework to evaluate the risk of open source components in use across Federal systems, and to study the potential for such an evaluation in private sector critical infrastructure. Additionally, the bill would establish a software security subcommittee on the CISA Cybersecurity Advisory Committee and require the Office of Manage-

ment and Budget (OMB) to issue guidance on the responsibilities of Federal agency chief information officers regarding open source software.[1]

II. Background and Need for the Legislation

Open source software is ubiquitous in modern information technology. Virtually every computer in the world, and every software application, contains open source software—it is one of the foundational building blocks of the modern digital world.[2] Due to its near universal use, a vulnerability affecting a widespread open source software component can be leveraged to attack millions of computers by bad actors, including Federal government systems, as evidenced by the significant public attention paid to the Log4Shell vulnerability.[3] In November 2021, researchers from the Chinese technology company Alibaba disclosed a vulnerability, called Log4Shell, affecting Log4j, a widely used open-source logging library for the Java programming language.[4] On December 10, 2021, the vulnerability was publicly disclosed, along with a patch that fixed the vulnerability.[5] The vulnerability allows attackers to easily execute arbitrary code on computers, effectively allowing an attacker to take full control over a system.[6] The Director of CISA, Jen Easterly, called Log4Shell "one of the most serious" vulnerabilities she had ever seen.[7] S. 917, the *Securing Open Source Software Act*, would help improve the secure use of open source software in the Federal government and critical infrastructure.

Open source software is software where the license (an open-source license) allows the source code to be reviewed, modified, and used by the public to customize it for their own purpose, often at no cost.[8] Much open source software is developed by not-for-profit entities—whether formally organized communities, loosely organized groups of developers, or individuals—though there are many exceptions.[9] It is collaboratively developed in a decentralized way and as a result is often cheaper, more flexible, and longer lasting than proprietary software.[10] Proprietary software can only be legally altered or copied by the original authors and used for the purposes specified in the license. Linux is an example of widely used open source software.[11]

---

[1] On September 28, 2022, the Committee approved S. 4938, the *Securing Open Source Software Act of 2022*. That bill is substantially similar to S. 917. Accordingly, this committee report is in many respects similar to the committee report for S. 4938. *See* S. Rept. No. 117–278.

[2] *The Digital Economy Runs on Open Source. Here's How to Protect It*., Harvard Business Review (Sept. 2, 2021) (https://hbr.org/2021/09/the-digital-economy-runs-on-open-source-heres-how-to-protect-it).

[3] *CISA warns 'most serious' Log4j vulnerability likely to affect hundreds of millions of devices*, CyberScoop (Dec. 13, 2021) (www.cyberscoop.com/log4j-cisa-easterly-most-serious/).

[4] Senate Committee on Homeland Security and Governmental Affairs, Statement of David Nalley, President of Apache Software Foundation, *Hearing on Responding to and Learning from the Log4Shell Vulnerability*, 117th Cong. (Feb. 8, 2022) (S. Hrg. 117–519).

[5] Cybersecurity and Infrastructure Security Agency, *Mitigating Log4Shell and Other Log4j-Related Vulnerabilities* (Dec. 2021) (www.cisa.gov/uscert/ncas/alerts/aa21-356a).

[6] *Id.*

[7] *CISA warns 'most serious' Log4j vulnerability likely to affect hundreds of millions of devices*, CyberScoop (Dec. 13, 2021) (www.cyberscoop.com/log4j-cisa-easterly-most-serious/).

[8] *What is open source?*, Red Hat (Oct. 24, 2019) (https://www.redhat.com/en/topics/open-source/what-is-open-source).

[9] *E.g.*, Google Open Source, https://opensource.google/.

[10] *What is open source?*, Red Hat (Oct. 24, 2019) (https://www.redhat.com/en/topics/open-source/what-is-open-source).

[11] *Id.*

Although some open source software is simply released for public use by the author and not maintained, other open source software may continue to have an official version that is maintained through organized communities of open-source software developers.[12] These communities are often facilitated by "foundations"—generally non-profit organizations run by volunteers who set rules and standards for any products that choose to be maintained under that foundation's umbrella.[13] An open source software developer can continue to maintain control over official versions and although anyone can download, modify, and use the source code for their own purposes, only developers who are approved by the project can modify and publish a new official version of the software. For example, the Apache Software Foundation facilitates about 650,000 people working on about 350 official products. Although anyone can download, modify, and use open source Apache software, including any of the 650,000 people working on the project, only about 8,300 of them have earned some level of status in the different project communities that allows them to implement changes to the official versions of code. Others can only propose changes, which are then reviewed by a core team. It can take months or years of work and the submission of more than 50 or 100 proposed changes (dependent on the Foundation's and project's own policies) before someone is granted the status to change the official code.[14]

Open source software code can be used like building blocks in larger software projects by developers for little to no cost.[15] As of early 2022, on average, an enterprise application has 384 open-source libraries, which saves significant development time and expense.[16] For example, keeping track of what software is doing, i.e., logging (the function of Log4j), is a commonly used function—most software applications need to perform this action.[17] Rather than having every software company develop, maintain, and upgrade this same function, open source software was created and made freely available for anyone to use.[18]

Open source software, as with any software, has security challenges. Certain practices, such as secure coding education and adoption of security practices, can help secure software, including open source software.[19] For instance, the majority of vulnerabilities in software today are caused by flaws related to memory access.[20] Shifting away from memory-unsafe programming languages, such as C and C++, and towards memory-safe programming languages, such as Rust, Python, and Java, can eliminate entire classes of

---

[12] *Id.*

[13] David Nalley, President, Apache Software Foundation, Interview with Senate Homeland Security and Governmental Affairs Staff (Jan. 14, 2022).

[14] *Id.*

[15] *Id.*

[16] Megan Stifel, Chief Strategy Officer, Institute for Security and Technology and Marc Rogers, Vice President of Cybersecurity Strategy, Okta, Inc., Interview with Senate Homeland Security and Governmental Affairs Staff (Jan. 14, 2022).

[17] David Nalley, President, Apache Software Foundation, Interview with Senate Homeland Security and Governmental Affairs Staff (Jan. 14, 2022).

[18] *What is open source?*, Red Hat, (Oct. 24, 2019), https://www.redhat.com/en/topics/open-source/what-is-open-source.

[19] Open Source Security Foundation, *The Open Source Software Security Mobilization Plan* (May 2022) (openssf.org/oss-security-mobilization-plan/).

[20] Internet Security Research Group, *What is memory safety and why does it matter?* (memorysafety.org/docs/memory-safety/) and National Security Agency, *Cybersecurity Information Sheet: Software Memory Safety* (Document No. U/OO/219936–22 | PP–22–1723) (Nov 2022) (https://media.defense.gov/2022/Nov/10/2003112742/-1/-1/0/CSI_SOFTWARE_MEMORY_SAFETY.PDF).

vulnerabilities.[21] This bill's framework for assessing the risk of open source components requires an evaluation of the use of such security practices in open source software components.

Following the announcement of the Log4Shell vulnerability, the Senate Homeland Security and Governmental Affairs Committee held a hearing investigating its impact.[22] During the hearing, experts testified on the importance of open source software and the need for the Federal government to aid in securing it.[23] Members of the panel made recommendations for improving the relationship between the government and the open source community, increasing the government's investment in securing software supply chains, and evaluating open source software security risk, which have been incorporated into this legislation.[24]

The Department of Homeland Security's (DHS) Cyber Safety Review Board (CSRB), established in President Biden's Executive Order on Improving the Nation's Cybersecurity, conducted an investigation into Log4Shell.[25] In its review, the CSRB found that Log4Shell is an "endemic vulnerability" and that the vulnerability will "remain in systems for many years to come."[26] Despite its pervasiveness and significant attempts at exploitation, the CSRB did not yet find any "significant" attacks on critical infrastructure systems leveraging the Log4j vulnerability.[27]

Open source community efforts such as the Open Source Security Foundation (OpenSSF), housed under the non-profit Linux Foundation, have been established to aid in securing open source software.[28] In 2022, the OpenSSF released the Open Source Software Security Mobilization Plan, outlining work streams to secure open source software, including replacing non-memory safe programming languages and conducting risk assessments for top open source software components.[29] This legislation would facilitate partnerships with such community efforts to ensure government systems are being effectively secured and that the government contributes to the security of open source software.

III. LEGISLATIVE HISTORY

Senator Gary Peters (D–MI) introduced S. 917, the *Securing Open Source Software Act of 2023*, on March 22, 2023, with original cosponsor Senator Josh Hawley (R–MO). The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs. The Committee considered S. 917 at a business meeting on

---

[21] *Id.*

[22] Senate Committee on Homeland Security and Governmental Affairs, *Hearing on Responding to and Learning from the Log4Shell Vulnerability*, 117th Cong. (Feb. 8, 2022) (S. Hrg. 117–519).

[23] *Id.*

[24] Senate Committee on Homeland Security and Governmental Affairs, Statements of Dr. Trey Herr, Director of Cyber Statecraft Initiative, Atlantic Council; Brad Arkin, Senior Vice President, Chief Security and Trust Officer, Cisco Systems; and David Nalley, President of Apache Software Foundation, *Hearing on Responding to and Learning from the Log4Shell Vulnerability*, 117th Cong. (Feb. 8, 2022) (S. Hrg. 117–519).

[25] Exec. Order No. 14028, 86 Fed. Reg. 26633 (May 12, 2021). *See also* The White House, *Executive Order on Improving the Nation's Cybersecurity* (May 12, 2021) (www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/).

[26] Cyber Safety Review Board, *Review of the December 2021 Log4j Event* (July 2022) (www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11–2022_508.pdf).

[27] *Id.*

[28] Open Source Security Foundation (openssf.org).

[29] Open Source Security Foundation, *The Open Source Software Security Mobilization Plan* (May 2022) (openssf.org/oss-security-mobilization-plan/).

March 29, 2023. The bill was ordered reported favorably by roll call vote of 11 yeas to 1 nay, with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Blumenthal, Lankford, Romney, Scott, and Hawley voting in the affirmative, and with Senator Paul voting in the negative. Senators Carper, Johnson, and Marshall voted yea by proxy, for the record only.

Consistent with Committee Rule 3(G), the Committee reports the bill with a technical amendment by mutual agreement of the Chairman and Ranking Member.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section establishes the short title of the bill as the "Securing Open Source Software Act of 2023."

Section 2. Findings

This section provides Congress's findings on the need for the legislation, including that the open source software ecosystem is crucial for the national security of the United States, and that the Federal government should play a supporting role in ensuring the long-term security of open source software.

Section 3. Open source software security duties

Subsection (a) paragraph (1) amends section 2220 of title XXII of the Homeland Security Act of 2002 to define the terms "open source software," "open source software community," and "open source software component."

Subsection (a) paragraph (2) amends section 2202(c) of title XXII of the Homeland Security Act by amending the responsibilities of the Director of the Cybersecurity and Infrastructure Security Agency (CISA) to include supporting the secure usage and deployment of software, including open source software, in the software development lifecycle at Federal agencies.

Subsection (a) paragraph (3) adds section 2220F to title XXII, which establishes the duties of the Director of CISA regarding open source software security.

Section 2220F, "Open source software security duties" (as added by this Act) includes the following:

Subsection (a) of section 2220F defines the term "software bill of materials."

Subsection (b) of section 2220F requires that the Director of CISA employ individuals who, to the greatest extent practicable, have expertise and experience participating in the open source software community.

Subsection (c) paragraph (1) of section 2220F establishes duties of the Director regarding open source software security, which include performing outreach and engagement to secure open source software, supporting Federal efforts to secure open source software, and serving as a public point of contact for the security of open source software.

Subsection (c) paragraph (2) of section 2220F requires the Director to conduct an assessment of critical open source software components. The Director must publish a framework to assess the risk of open source software components, incorporating government, in-

dustry, and open source software community frameworks and best practices. The Director must determine every year whether updates to the framework are needed, including augmenting, adding, or removing elements from the framework. In developing the framework, the Director must consult with open source community members and Federal agencies, and must ensure to the greatest extent practicable that the framework is usable by the open source software community.

It also directs the Director to perform an assessment of the most critical open source software components used within the Federal government, using the established framework and information available at the time of the assessment. The Director must automate the assessment to the greatest extent practicable, publish tools developed to conduct the assessment, and share results of the assessment with appropriate entities.

It further requires the Director to study the feasibility of conducting the assessment for critical infrastructure entities. If the Director determines the assessment to be feasible, the Director may conduct a voluntary pilot assessment to last no more than 2 years with one or more critical infrastructure sectors. The Director must submit a report to Congress following the study and the pilot, to include any recommendations for continuing the activities carried out under the pilot, subsequent to termination of the pilot.

Subsection (c) paragraph (3) of section 2220F requires the Director to brief and coordinate with the National Cyber Director.

Subsection (c) paragraph (4) of section 2220F requires the Director to report to Congress not later than 1 year after the date of enactment, and every 2 years thereafter. The Director must make a version of these reports publicly available.

Subsection (b) contains technical and conforming amendments.

Section 4. Software security advisory subcommittee

This section amends section 2219 of title XXII of the Homeland Security Act of 2002 by adding a subcommittee on software security, including open source software security, to the CISA Cybersecurity Advisory Committee.

Section 5. Open source software guidance

Subsection (a) defines the term "Director" to mean the Director of the Office of Management and Budget (OMB). It defines the terms "open source software" and "open source software community" to have the meaning given in this Act. The section also defines the terms "appropriate congressional committee" and "covered agency."

Subsection (b) requires the Director of OMB to issue guidance on the responsibilities of the chief information officer at each covered agency regarding open source software. This guidance includes how chief information officers should manage and reduce risks of using open source software, guide contributing to and releasing open source software, and enable the secure usage of open source software. National security systems are exempt from such guidance.

Subsection (c) establishes a pilot, lasting no more than 4 years, to establish open source functions at between 1 and 5 covered agencies. The pilot functions must be modeled after existing non-Federal open source program offices, and support the secure usage of

open source software at the covered agency. Following the establishment of the pilot, the Director of OMB must assess whether such functions should be established at some or all covered agencies. If so, the Director must issue guidance on the implementation of those functions.

Subsection (d) requires the Director of OMB to brief Congress on the guidance and issue a report on the pilot open source functions.

Subsection (e) amends Section 3554 of title 44, United States Code, to include the secure usage and development of software, including open source software, in the information security responsibilities of Federal agencies.

Section 6. Rule of construction

This section states that nothing in this Act or the amendments made by this Act shall be construed to provide any additional regulatory authority to any agency described therein.

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. Congressional Budget Office Cost Estimate

At a Glance

S. 917, Securing Open Source Software Act of 2023

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on March 29, 2023

By Fiscal Year, Millions of Dollars	2023	2023-2028	2023-2033
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	52	not estimated

Increases *net direct spending* in any of the four consecutive 10-year periods beginning in 2034?	No	Statutory pay-as-you-go procedures apply?	No
		Mandate Effects	
Increases *on-budget deficits* in any of the four consecutive 10-year periods beginning in 2034?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

The bill would:

- Require assessments of open-source software used by federal agencies
- Establish a pilot program to assess open-source software security at federal agencies

- Direct the Cybersecurity and Infrastructure Security Agency to hire open-source software analysts
- Require several reports and studies about the effectiveness of open-source software assessments

Estimated budgetary effects would mainly stem from:

- Testing information systems for open-source software vulnerabilities
- Assessing federal network security
- Hiring open-source software analysts

Areas of significant uncertainty include:

- Predicting staffing requirements of federal open-source program offices
- Anticipating the contract costs of software assessments

Bill summary: S. 917 would authorize the Cybersecurity and Infrastructure Security Agency (CISA) to improve the security of open-source software, or computer code that is publicly available for anyone to use or modify. The bill would require the agency to identify and mitigate vulnerabilities in open-source software used by federal agencies. Under the bill, CISA would conduct annual assessments of the security of commonly used open-source software.

S. 917 also would establish a pilot program to study the operations of open-source software program offices within participating federal agencies. The bill would direct such agencies to develop policies for the safe deployment and management of open-source software on their information networks.

Estimated Federal cost: The estimated budgetary effects of S. 917 are shown in Table 1.

TABLE 1.—ESTIMATED BUDGETARY EFFECTS OF S. 917

	By fiscal year, millions of dollars—						
	2023	2024	2025	2026	2027	2028	2023–2028
Open-Source Software Assessments:							
Estimated Authorization	0	0	6	6	6	6	24
Estimated Outlays	0	0	6	6	6	6	24
CISA Open-Source Staff:							
Estimated Authorization	0	2	4	4	4	4	18
Estimated Outlays	0	2	4	4	4	4	18
Open-Source Program Offices:							
Estimated Authorization	0	1	3	3	3	0	10
Estimated Outlays	0	1	3	3	3	0	10
Total Changes:							
Estimated Authorization	0	3	13	13	13	10	52
Estimated Outlays	0	3	13	13	13	10	52

Basis of estimate: For this estimate, CBO assumes that S. 917 will be enacted in 2023 and that CISA would begin to implement most of the bill's requirements in 2025.

CBO expects that the costs to implement S. 917 would include the salaries and benefits of additional federal staff and procurement of new software. Outlays are based on historical spending patterns for existing or similar programs.

Spending subject to appropriation: CBO estimates that implementing the bill would cost $52 million over the 2023–2028 period. Such spending would be subject to the availability of appropriated funds.

Open-source software assessments: CISA currently operates programs to identify and mitigate threats to federal information systems. S. 917 would require CISA to assess open-source software used by the federal government for security vulnerabilities. Under the bill, CISA would review the supply chain histories of open-source applications to identify any potential cybersecurity vulnerabilities in the underlying code. CISA would be required to share its findings so that software users could remediate any weaknesses.

Using information from CISA, CBO expects that the agency would implement this program by procuring new software and tools capable of scanning for vulnerabilities in open-source code used by federal agencies. On the basis of similar acquisition programs, CBO estimates that the cost to acquire and annually update those tools would total $24 million over the 2023–2028 period.

CISA open-source staff: S. 917 would require CISA to publish a framework for the secure adoption and management of open-source software in the information networks and devices of federal, state, and private-sector entities. CISA also would provide information about vulnerabilities in open-source software. CBO anticipates that the framework and vulnerability assessments would be updated annually. CBO expects that CISA would need 20 open-source software analysts beginning in 2024 at an average annual cost of about $175,000 per employee. On that basis and accounting for the effects of anticipated inflation, CBO estimates that salaries and benefits of those employees would total $18 million over the 2023–2028 period.

Open-source program offices: S. 917 would require the Administration to establish a pilot program where up to five federal agencies would establish new offices to manage the use of secure open-source software. CBO expects that three agencies would participate in the pilot program and that participating agencies would each require on average five analysts to develop policies, share best practices, and monitor open-source applications. CBO estimates that compensation would average about $175,000 annually and that agencies would begin hiring those employees in 2024. Under the bill, the pilot program would terminate after four years. On that basis and accounting for the effects of anticipated inflation, CBO estimates that salaries and benefits of those employees would total $10million over the 2023–2028 period.

Uncertainty: Areas of uncertainty in this estimate include predicting the acquisition timeline to support assessments at federal agencies and critical infrastructure operators. CBO anticipates that CISA would be able to procure and deploy the necessary software to assess federal open-source software in the 2023–2028 period. The budgetary effects of the bill could be millions of dollars higher or lower than CBO's estimate if the time needed to deploy these tools differs from CBO's estimate.

The budgetary effects of the bill also would depend on accurately predicting the number of additional employees that would be needed at CISA and other federal agencies to satisfy the requirements of the bill. Costs would be moderately larger or smaller than this estimate depending on how the number of hired analysts differs from CBO's estimate.

Pay-As-You-Go considerations: None.

Increase in long-term net direct spending and deficits: None.
Mandates: None.
Estimate prepared by: Federal costs: Aldo Prosperi; Mandates: Brandon Lever.
Estimate reviewed by: David Newman, Chief, Defense, International Affairs, and Veterans' Affairs Cost Estimates Unit; Kathleen FitzGerald, Chief, Public and Private Mandates Unit; Chad Chirico, Deputy Director of Budget Analysis.
Estimate approved by: Phillip L. Swagel, Director, Congressional Budget Office.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

* * * * * * *

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Sec. 2220F. Open source software security duties.

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

SEC. 2200. DEFINITIONS.

* * * * * * *

(21) * * *

(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.

[(22)**]***(25)* * * *

[(23)**]***(26)* * * *

[(24)**]***(27)* * * *

[(25)**]***(28)* * * *

[(26)**]***(29)* * * *

[(27)**]***(30)* * * *

[(28)**]***(31)* * * *

* * * * * * *

SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) * * *

(b) * * *

(c) * * *

* * * * * * *

(13) carry out the duties and authorities relating to the.gov internet domain, as described in section 2215; **[**and**]**

(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

[(14)**]***(15)* * * *

* * * * * * *

SEC 2219. CYBERSECURITY ADVISORY COMMITTEE.

* * * * * * *

(d) * * *

(1) * * *

(A) * * *

* * * * * * *

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

* * * * * * *

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, and the open source software community; and

(E) support Federal and non-Federal supply chain security efforts by encouraging efforts to bolster open source 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, including those published by the National Institute of Standards and Technology, industry, and open source software community frameworks and best practices, 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 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 an 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 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 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 (2)(B) since the last report submitted under this subparagraph;

(iv) a summary of 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 an assessment conducted pursuant to paragraph (2)(E) since the last report 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.

* * * * * * *

UNITED STATES CODE

* * * * * * *

TITLE 44—PUBLIC PRINTING AND DOCUMENTS

* * * * * * *

CHAPTER 35—COORDINATION OF FEDERAL INFORMATION POLICY

* * * * * * *

Subchapter II—Information Security

* * * * * * *

SEC. 3554. FEDERAL AGENCY RESPONSIBILITIES.

(a) * * *

(b) * * *

* * * * * * *

(7) * * *

* * * * * * *

(C) * * *

(i) * * *

(ii) * * *

(iii) * * *

* * * * * * *

(IV) any other agency or office, in accordance with law or as directed by the President;[and]

(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency**[**.**]***; and*

(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)).

* * * * * * *

○