118TH CONGRESS
*1st Session*
HOUSE OF REPRESENTATIVES
REPT. 118–160
Part 1

# SECURING OPEN SOURCE SOFTWARE ACT OF 2023

JULY 27, 2023.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. GREEN of Tennessee, from the Committee on Homeland Security, submitted the following

# R E P O R T

[To accompany H.R. 3286]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (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, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS



The amendment is as follows:

Strike all after the enacting clause and insert the following:

**SECTION 1. SHORT TITLE.**

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

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

(a) IN GENERAL.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 650 et seq.) is amended—

(1) in section 2200 (6 U.S.C. 650)—

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

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

"(22) OPEN SOURCE SOFTWARE.—The term 'open source software' means software for which the human-readable source code is made available to the public for use, study, re-use, modification, enhancement, and re-distribution.

"(23) OPEN SOURCE SOFTWARE COMMUNITY.—The term 'open source software community' means the community of individuals, foundations, nonprofit organizations, corporations, and other entities that—

"(A) develop, contribute to, maintain, and publish open source software; or

"(B) otherwise work to ensure the security of the open source software ecosystem.

"(24) OPEN SOURCE SOFTWARE COMPONENT.—The term 'open source software component' means an individual repository of open source software that is made available to the public.";

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

(A) in paragraph (13), by striking "and" at the end;

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

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

"(14) support, including by offering services, the secure usage and deployment of software, including open source software, in the software development lifecycle at Federal agencies in accordance with section 2220F; and"; and

(3) by adding at the end the following:

**"SEC. 2220F. OPEN SOURCE SOFTWARE SECURITY DUTIES.**

"(a) DEFINITION.—In this section, the term 'software bill of materials' has the meaning given such term in the Minimum Elements for a Software Bill of Materials published by the Department of Commerce, or any superseding definition published by the Agency.

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

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

"(2) perform the duties described in subsection (c).

"(c) DUTIES OF THE DIRECTOR.—

"(1) IN GENERAL.—The Director shall—

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

"(B) support Federal efforts to strengthen the security of open source software;

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

"(D) serve as a public point of contact regarding the security of open source software for non-Federal entities, including State, local, Tribal, and territorial partners, the private sector, international partners, and open source software communities; and

"(E) support Federal and non-Federal supply chain security efforts by encouraging efforts to bolster open source software security, such as—

"(i) assisting in coordinated vulnerability disclosures in open source software components pursuant to section 2209(n); and

"(ii) supporting the activities of the Federal Acquisition Security Council.

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

"(A) FRAMEWORK.—Not later than one year after the date of the enactment of this section, the Director shall publicly publish a framework, incorporating government, private sector, and open source software community frameworks and best practices, including those published by the National Institute of Standards and Technology, for assessing the risk of open source software components, including direct and indirect open source software dependencies, which shall incorporate, at a minimum, the following with respect to a given open source software component:

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

"(ii) The security practices of development, build, and release processes, such as the use of multi-factor authentication by maintainers and cryptographic signing of releases.

"(iii) The number and severity of publicly known, unpatched vulnerabilities.

"(iv) The breadth of deployment.

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

"(vi) The health and sustainability of the open source software community, including, where applicable, the level of current and historical investment and maintenance in such component, such as the number and activity of individual maintainers.

"(B) UPDATING FRAMEWORK.—Not less frequently than annually after the date on which the framework is published under subparagraph (A), the Director shall—

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

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

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

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

"(ii) The open source software community.

"(D) USABILITY.—The Director shall ensure, to the greatest extent practicable, that the framework described in subparagraph (A) is usable by the open source software community, including through the consultation required under subparagraph (C).

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

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

"(I) software bills of material that are, at the time of the assessment, made available to the Agency or are otherwise accessible via the internet;

"(II) software inventories, available to the Director at the time of the assessment, from the Continuous Diagnostics and Mitigation program of the Agency; and

"(III) other publicly available information regarding open source software components; and

"(ii) develop, in consultation with the Federal agency at which an open source software component is deployed, one or more ranked lists of components described in clause (i) based on such assessment, such as ranked by the criticality, level of risk, or usage of the components, or a combination thereof.

"(F) AUTOMATION.—The Director shall, to the greatest extent practicable, automate the assessment performed pursuant to subparagraph (E).

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

"(H) SHARING.—

"(i) RESULTS.—The Director, to the greatest extent practicable, and taking into account the sensitivity of the information contained in the assessment performed pursuant to subparagraph (E), shall facilitate the sharing of the results of each assessment under subparagraph (E)(i) with appropriate Federal and non-Federal entities working to support the security of open source software, including by offering means for appropriate Federal and non-Federal entities to download the assessment in an automated manner.

"(ii) DATASETS.—The Director may publicly publish, as appropriate, any datasets or versions of the datasets developed or consolidated as a result of an assessment under subparagraph (E)(i).

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

"(i) STUDY.—Not later than two years after the publication of the framework under subparagraph (A), the Director shall conduct a study regarding the feasibility of the Director conducting the assessment under subparagraph (E) for critical infrastructure entities.

"(ii) PILOT.—

"(I) IN GENERAL.—If the Director determines that the assessment described in clause (i) is feasible, the Director may conduct a pilot assessment on a voluntary basis with one or more critical infrastructure sectors, in coordination with the Sector Risk Management Agency and the sector coordinating council of each participating sector.

"(II) TERMINATION.—If the Director proceeds with the pilot assessment described in subclause (I), such pilot assessment shall terminate not later than two years after the date on which the Director begins such pilot assessment.

"(iii) REPORTS.—

"(I) STUDY.—Not later than 180 days after the date on which the Director completes the study conducted under clause (i), the Director shall submit to the appropriate congressional committees a report that—

"(aa) summarizes the study;

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

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

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

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

"(II) PILOT.—If the Director proceeds with the pilot assessment described in clause (ii), not later than one year after the date on which the Director begins such pilot assessment, the Director shall submit to the appropriate congressional committees a report that includes the following:

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

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

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

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

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

"(4) REPORTS.—

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

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

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

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

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

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

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

"(B) PUBLIC REPORT.—Not later than 30 days after the date on which the Director submits each report required under subparagraph (A), the Director shall make a version of each such report publicly available on the website of the Agency.".

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

"Sec. 2220F. Open source software security duties.".

(c) SOFTWARE SECURITY ADVISORY SUBCOMMITTEE.—Section 2219(d)(1) of the Homeland Security Act of 2002 (6 U.S.C. 665e(d)(1)) is amended by adding at the end the following:

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

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

## PURPOSE AND SUMMARY

Open source software is a critical part of our digital infrastructure. A secure, healthy, vibrant, and resilient open source software ecosystem is crucial for ensuring the national security and economic vitality of the United States. However, due to both the unique strengths of open source software and inconsistent historical investment in open source software security, there exist unique challenges in securing open source software.

H.R. 3286 requires the Cybersecurity and Infrastructure Security Agency (CISA) to publish a framework to assess the most critical open source software libraries used in the Federal government and requires CISA to assess the feasibility of creating a voluntary pilot program to assess open source software usage across critical infrastructure. The bill also requires CISA to hire from and build relationships with the open source community to help mitigate vulnerabilities like the one in Log4j and allow the Federal government to more swiftly response when vulnerabilities are discovered.

## BACKGROUND AND NEED FOR LEGISLATION

Open source software is the bedrock of the digital ecosystem. Virtually every computer in the world relies on open source code that is distributed for free and maintained by the open source community, consisting of a group of individuals and organizations that develop and maintain open source software.

The collaborative nature of open source software offers opportunities for innovation and societal advancement, but also poses security challenges, as highlighted by the Log4j vulnerability's impact on millions of computers worldwide. Log4j is a very widely used piece of open source software. In December 2021, a new vulnerability, called a zero day, was discovered within Log4j, resulting in cyber risk to millions of devices across the globe. At the time, cyber professionals described the vulnerability as the worst many had seen in their careers.

The *Securing Open Source Software Act of 2023* is a direct response to the threats posed by the Log4j vulnerability. This bill aims to address these security challenges by authorizing a number of activities at the Cybersecurity and Infrastructure Security Agency (CISA) to support the security of open source software. The Federal government is one of the largest users of open source software in the world and must both manage its own risk and, in turn, contribute back to the security of open source software. The framework

required in the *Securing Open Source Software Act of 2023* will be used by CISA to evaluate the government's posture and better position federal agencies to securely use open source software. While use of the framework is voluntary for the private sector, the bill requires CISA to conduct a study and consider a voluntary pilot program to assess the open source software components used in critical infrastructure. These steps will allow CISA and public and private sector partners to assess, manage, and reduce risks to support the secure usage of open source software.

## HEARINGS

The Committee held the following hearing in the 118th Congress that informed H.R. 3286:

On April 27, 2023, the Subcommittee on Cybersecurity and Infrastructure Protection held a hearing entitled "CISA 2025: The State of American Cybersecurity from CISA's Perspective." The Subcommittee received testimony from the Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency.

## COMMITTEE CONSIDERATION

The Committee met on May 17, 2023, a quorum being present, to consider H.R. 3286 and ordered the measure to be favorably reported to the House, as amended, by voice vote.

## COMMITTEE VOTES

Clause 3(b) of rule XIII requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 3286.

## COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X, are incorporated in the descriptive portions of this report.

## CORRESPONDENCE WITH OTHER COMMITTEES

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY,
*Washington, DC, July 18, 2023.*

Hon. MARK GREEN,
*Chairman, Committee on Homeland Security,*
*Washington, DC.*

DEAR CHAIRMAN GREEN: I write concerning H.R. 3286, the Securing Open Source Software Act of 2023. This bill contains provisions within the jurisdiction of the House Committee on Oversight and Accountability. As a result of your having consulted with me concerning the provisions of the bill that fall within our Rule X jurisdiction, I agree to forgo consideration of the bill, so the bill may proceed expeditiously to the House floor.

The Committee takes this action with our mutual understanding that by foregoing consideration of H.R. 3286 we do not waive any

jurisdiction over the subject matter contained in this or similar legislation, and we will be appropriately consulted and involved as the bill or similar legislation moves forward so we may address any remaining issues within our Rule X jurisdiction. The House Committee on Oversight and Accountability also reserves the right to seek appointment of an appropriate number of conferees to any House-Senate conference involving this or similar legislation and requests your support of any such request.

Finally, I would ask that a copy of our exchange of letters on this matter be included in the bill report filed by the Committee on Oversight and Accountability. I appreciate your commitment to also include these letters in the *Congressional Record* during floor consideration of H.R. 3286.

Sincerely,

JAMES COMER,
*Chairman, House Committee on Oversight and Accountability.*

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
*Washington, DC, July 18, 2023.*

Hon. JAMES COMER,
*Chairman, Committee on Oversight and Accountability,*
*Washington, DC.*

DEAR CHAIRMAN COMER: Thank you for your letter regarding H.R. 3286, the "Securing Open Source Software Act of 2023," of which the Committee on Oversight and Accountability received an additional referral. I appreciate your support in bringing this legislation before the House of Representatives, and that the Committee on Oversight and Accountability will forego further consideration of the bill.

The Committee on Homeland Security concurs with the mutual understanding that by foregoing consideration of this bill at this time, the Committee on Oversight and Accountability does not waive jurisdiction over the subject matter contained in this legislation in the future. In addition, should a conference on this bill be necessary, I would support your request to have the Committee on the Oversight and Accountability represented on the conference committee.

I will include our letters on H.R. 3286 in the Committee report on this measure and in the *Congressional Record* during floor consideration of this bill. I look forward to working with you on this legislation and appreciate your cooperation on this matter.

Sincerely,

MARK E. GREEN, MD,
*Chairman.*

## CONGRESSIONAL BUDGET OFFICE ESTIMATE, NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c) of rule XIII and section 308(a) of the Congressional Budget Act of 1974, and with respect to the requirements of clause 3(c)(3) of rule XIII and section 402 of the Congressional Budget Act of 1974, the Committee adopts as its own the estimate of any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or

tax expenditures contained in the cost estimate prepared by the Director of the Congressional Budget Office.

Insert offset folio 14 here HR160.001

The bill would

- Require assessments of open-source software used by 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

- Anticipating the contract costs of software assessments
- Predicting staffing requirements

Bill summary: H.R. 3286 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.

Estimated Federal cost: The estimated budgetary effects of H.R. 3286 are shown in Table 1. The costs of the legislation fall within budget function 050 (national defense).

TABLE 1.—ESTIMATED BUDGETARY EFFECTS OF H.R. 3286

| | 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 |

TABLE 1.—ESTIMATED BUDGETARY EFFECTS OF H.R. 3286—Continued

| | By fiscal year, millions of dollars— | | | | | | |
|---|---|---|---|---|---|---|---|
| | 2023 | 2024 | 2025 | 2026 | 2027 | 2028 | 2023–2028 |
| CISA Open-Source Staff | | | | | | | |
| Estimated Authorization | 0 | 2 | 4 | 4 | 4 | 4 | 18 |
| Estimated Outlays | 0 | 2 | 4 | 4 | 4 | 4 | 18 |
| Total Changes | | | | | | | |
| Estimated Authorization | 0 | 2 | 10 | 10 | 10 | 10 | 42 |
| Estimated Outlays | 0 | 2 | 10 | 10 | 10 | 10 | 42 |

Basis of estimate: For this estimate, CBO assumes that H.R. 3286 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 H.R. 3286 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 $42 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. H.R. 3286 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. H.R. 3286 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.

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 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.

Previous CBO estimate: On April 6, 2023, CBO transmitted a cost estimate for S. 917, the Securing Open Source Software Act of 2023, as ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on March 29, 2023. The estimated cost of S. 917 is higher than the cost of H.R. 3286 because the former bill would authorize a federal pilot program that would not be authorized by the latter.

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.

PHILLIP L. SWAGEL,
*Director, Congressional Budget Office.*

## FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act of 1995.

## DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 3286 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

## STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the objective of H.R. 3286 is to require CISA to undertake certain responsibilities to ensure the security of open source software use in the Federal government.

## CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with rule XXI, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of rule XXI.

## ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act (5 U.S.C. § 1004) were created by this legislation.

## APPLICABILITY TO THE LEGISLATIVE BRANCH

The Committee finds that H.R. 3286 does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

## SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

*Section 1. Short title*

This section designates the name of the bill as the "Securing Open Source Software Act of 2023".

*Section 2. Open source software duties*

Subsection (a) amends section 2201 of Subtitle A 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".

This subsection also amends section 2202 of Subtitle A 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.

This subsection also adds Section 2220F of Subtitle A of title XXII, which establishes the duties of the Director of CISA regarding open source software security.

*Section 2220F:*

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

Subsection (b) requires that the Director employs individuals who, to the greatest extent practicable, have expertise and experience participating in the open source software community.

Subsection (c) establishes duties of the Director regarding open source software security, which includes 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) also 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, industry, and open source software community frameworks and best practices. The Director must determine every year whether updates to the framework are needed. In developing the framework, the Director must consult with open source community members and Federal agencies.

Subsection (c) then directs the Director to perform an assessment of the most critical open source software components used on high-value assets, as defined by Office of Management and Budget Memorandum M–19–03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program*, using the established framework. The Director shall automate the assessment to the greatest extent practicable. The Director shall publish tools developed to conduct the as-

sessment and shall share the results of the assessment with appropriate entities.

Subsection (c) also directs 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 with 1 or more critical infrastructure sectors. The Director shall submit a report to Congress following the study and the pilot. If the Director conducts the pilot, the pilot shall be sunset 2 years after the commencement of the pilot.

Subsection (c) requires the Director to report to Congress not later than 1 year after the date of enactment of the section, and every 2 years thereafter for the next seven years. The Director shall make a version of such reports publicly available.

Subsection (c) also requires the Director to brief and consult with the National Cyber Director, as appropriate.

Subsection (b) amends the table of contents to insert the new section 2220F, as added by Subsection (a).

Subsection (c) authorizes CISA to create a subcommittee on software security, including open source software security, to the CISA Cybersecurity Advisory Committee.

Subsection (d) 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.

## CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, 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.**

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

# TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

## Subtitle A—Cybersecurity and Infrastructure Security

**SEC. 2200. DEFINITIONS.**

Except as otherwise specifically provided, in this title:

(1) AGENCY.—The term "Agency" means the Cybersecurity and Infrastructure Security Agency.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Homeland Security of the House of Representatives.

(3) CLOUD SERVICE PROVIDER.—The term "cloud service provider" means an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in NIST Special Publication 800–145 and any amendatory or superseding document relating thereto.

(4) CRITICAL INFRASTRUCTURE INFORMATION.—The term "critical infrastructure information" means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

(5) CYBER THREAT INDICATOR.—The term "cyber threat indicator" means information that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for

the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(H) any combination thereof.

(6) CYBERSECURITY PURPOSE.—The term "cybersecurity purpose" means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

(7) CYBERSECURITY RISK.—The term "cybersecurity risk"—

(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(8) CYBERSECURITY THREAT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term "cybersecurity threat" means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) EXCLUSION.—The term "cybersecurity threat" does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(9) DEFENSIVE MEASURE.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term "defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that de-

tects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

(B) EXCLUSION.—The term "defensive measure" does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

(i) the private entity, as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501), operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

(10) DIRECTOR.—The term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency.

(11) HOMELAND SECURITY ENTERPRISE.—The term "Homeland Security Enterprise" means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and Tribal government officials, private sector representatives, academics, and other policy experts.

(12) INCIDENT.—The term "incident" means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

(13) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term "Information Sharing and Analysis Organization" means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of an interference, a compromise, or an incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

(14) INFORMATION SYSTEM.—The term "information system"—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

(15) INTELLIGENCE COMMUNITY.—The term "intelligence community" has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(16) MALICIOUS CYBER COMMAND AND CONTROL.—The term "malicious cyber command and control" means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

(17) MALICIOUS RECONNAISSANCE.—The term "malicious reconnaissance" a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(18) MANAGED SERVICE PROVIDER.—The term "managed service provider" means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.

(19) MONITOR.—The term "monitor" means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

(20) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term "national cybersecurity asset response activities" means—

(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

(D) facilitating information sharing and operational coordination with threat response; and

(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

(21) NATIONAL SECURITY SYSTEM.—The term "national security system" has the meaning given the term in section 11103 of title 40, United States Code.

*(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)* RANSOMWARE ATTACK.—The term "ransomware attack"—

(A) means an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

(B) does not include any such event in which the demand for payment is—

(i) not genuine; or

(ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system.

**[**(23)**]** *(26)* SECTOR RISK MANAGEMENT AGENCY.—The term "Sector Risk Management Agency" means a Federal department or agency, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

**[**(24)**]** *(27)* SECURITY CONTROL.—The term "security control" means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

**[**(25)**]** *(28)* SECURITY VULNERABILITY.—The term "security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

**[**(26)**]** *(29)* SHARING.—The term "sharing" (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).

**[**(27)**]** *(30)* SLTT ENTITY.—The term "SLTT entity" means a domestic government entity that is a State government, local government, Tribal government, territorial government, or any subdivision thereof.

**[**(28)**]** *(31)* SUPPLY CHAIN COMPROMISE.—The term "supply chain compromise" means an incident within the supply chain of an information system that an adversary can leverage, or does leverage, to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.

**SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.**

(a) REDESIGNATION.—

(1) IN GENERAL.—The National Protection and Programs Directorate of the Department shall, on and after the date of the enactment of this subtitle, be known as the "Cybersecurity and Infrastructure Security Agency".

(2) REFERENCES.—Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Security Agency of the Department.

(b) DIRECTOR.—

(1) IN GENERAL.—The Agency shall be headed by the Director, who shall report to the Secretary.

(2) QUALIFICATIONS.—

(A) IN GENERAL.—The Director shall be appointed from among individuals who have—

(i) extensive knowledge in at least two of the areas specified in subparagraph (B); and

(ii) not fewer than five years of demonstrated experience in efforts to foster coordination and collaboration between the Federal Government, the private sector, and other entities on issues related to cybersecurity, infrastructure security, or security risk management.

(B) SPECIFIED AREAS.—The areas specified in this subparagraph are the following:

(i) Cybersecurity.

(ii) Infrastructure security.

(iii) Security risk management.

(3) REFERENCE.—Any reference to an Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and any other related program of the Department as described in section 103(a)(1)(H) as in effect on the day before the date of enactment of this subtitle in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Director of the Cybersecurity and Infrastructure Security Agency.

(c) RESPONSIBILITIES.—The Director shall—

(1) lead cybersecurity and critical infrastructure security programs, operations, and associated policy for the Agency, including national cybersecurity asset response activities;

(2) coordinate with Federal entities, including Sector-Specific Agencies, and non-Federal entities, including international entities, to carry out the cybersecurity and critical infrastructure activities of the Agency, as appropriate;

(3) carry out the responsibilities of the Secretary to secure Federal information and information systems consistent with law, including subchapter II of chapter 35 of title 44, United States Code, and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113)), including by carrying out a periodic strategic assessment of the related programs and activities of the Agency to ensure such programs and activities contemplate the in-

novation of information systems and changes in cybersecurity risks and cybersecurity threats;

(4) coordinate a national effort to secure and protect against critical infrastructure risks, consistent with subsection (e)(1)(E);

(5) upon request, provide analyses, expertise, and other technical assistance to critical infrastructure owners and operators and, where appropriate, provide those analyses, expertise, and other technical assistance in coordination with Sector-Specific Agencies and other Federal departments and agencies;

(6) develop and utilize mechanisms for active and frequent collaboration between the Agency and Sector-Specific Agencies to ensure appropriate coordination, situational awareness, and communications with Sector-Specific Agencies;

(7) maintain and utilize mechanisms for the regular and ongoing consultation and collaboration among the Divisions of the Agency to further operational coordination, integrated situational awareness, and improved integration across the Agency in accordance with this Act;

(8) develop, coordinate, and implement—

(A) comprehensive strategic plans for the activities of the Agency; and

(B) risk assessments by and for the Agency;

(9) carry out emergency communications responsibilities, in accordance with title XVIII;

(10) carry out cybersecurity, infrastructure security, and emergency communications stakeholder outreach and engagement and coordinate that outreach and engagement with critical infrastructure Sector-Specific Agencies, as appropriate;

(11) provide education, training, and capacity development to Federal and non-Federal entities to enhance the security and resiliency of domestic and global cybersecurity and infrastructure security;

(12) appoint a Cybersecurity State Coordinator in each State, as described in section 2217;

(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)* carry out such other duties and powers prescribed by law or delegated by the Secretary.

(d) DEPUTY DIRECTOR.—There shall be in the Agency a Deputy Director of the Cybersecurity and Infrastructure Security Agency who shall—

(1) assist the Director in the management of the Agency; and

(2) report to the Director.

(e) CYBERSECURITY AND INFRASTRUCTURE SECURITY AUTHORITIES OF THE SECRETARY.—

(1) IN GENERAL.—The responsibilities of the Secretary relating to cybersecurity and infrastructure security shall include the following:

(A) To access, receive, and analyze law enforcement information, intelligence information, and other information

from Federal Government agencies, State, local, tribal, and territorial government agencies, including law enforcement agencies, and private sector entities, and to integrate that information, in support of the mission responsibilities of the Department, in order to—

(i) identify and assess the nature and scope of terrorist threats to the homeland;

(ii) detect and identify threats of terrorism against the United States; and

(iii) understand those threats in light of actual and potential vulnerabilities of the homeland.

(B) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States, including an assessment of the probability of success of those attacks and the feasibility and potential efficacy of various countermeasures to those attacks. At the discretion of the Secretary, such assessments may be carried out in coordination with Sector-Specific Agencies.

(C) To integrate relevant information, analysis, and vulnerability assessments, regardless of whether the information, analysis, or assessments are provided or produced by the Department, in order to make recommendations, including prioritization, for protective and support measures by the Department, other Federal Government agencies, State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities regarding terrorist and other threats to homeland security.

(D) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this title, including obtaining that information from other Federal Government agencies.

(E) To develop, in coordination with the Sector-Specific Agencies with available expertise, a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency communications systems, and the physical and technological assets that support those systems.

(F) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other Federal Government agencies, including Sector-Specific Agencies, and in cooperation with State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities.

(G) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information relating to homeland security within the Federal Government and between Federal Govern-

ment agencies and State, local, tribal, and territorial government agencies and authorities.

(H) To disseminate, as appropriate, information analyzed by the Department within the Department to other Federal Government agencies with responsibilities relating to homeland security and to State, local, tribal, and territorial government agencies and private sector entities with those responsibilities in order to assist in the deterrence, prevention, or preemption of, or response to, terrorist attacks against the United States.

(I) To consult with State, local, tribal, and territorial government agencies and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

(J) To ensure that any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties.

(K) To request additional information from other Federal Government agencies, State, local, tribal, and territorial government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

(L) To establish and utilize, in conjunction with the Chief Information Officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

(M) To coordinate training and other support to the elements and personnel of the Department, other Federal Government agencies, and State, local, tribal, and territorial government agencies that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

(N) To coordinate with Federal, State, local, tribal, and territorial law enforcement agencies, and the private sector, as appropriate.

(O) To exercise the authorities and oversight of the functions, personnel, assets, and liabilities of those components transferred to the Department pursuant to section 201(g).

(P) To carry out the functions of the national cybersecurity and communications integration center under section 2209.

(Q) To carry out the requirements of the Chemical Facility Anti-Terrorism Standards Program established under title XXI and the secure handling of ammonium nitrate

program established under subtitle J of title VIII, or any successor programs.

(R) To encourage and build cybersecurity awareness and competency across the United States and to develop, attract, and retain the cybersecurity workforce necessary for the cybersecurity related missions of the Department, including by—

(i) overseeing elementary and secondary cybersecurity education and awareness related programs at the Agency;

(ii) leading efforts to develop, attract, and retain the cybersecurity workforce necessary for the cybersecurity related missions of the Department;

(iii) encouraging and building cybersecurity awareness and competency across the United States; and

(iv) carrying out cybersecurity related workforce development activities, including through—

(I) increasing the pipeline of future cybersecurity professionals through programs focused on elementary and secondary education, postsecondary education, and workforce development; and

(II) building awareness of and competency in cybersecurity across the civilian Federal Government workforce.

(2) REALLOCATION.—The Secretary may reallocate within the Agency the functions specified in sections 2203(b) and 2204(b), consistent with the responsibilities provided in paragraph (1), upon certifying to and briefing the appropriate congressional committees, and making available to the public, at least 60 days prior to the reallocation that the reallocation is necessary for carrying out the activities of the Agency.

(3) STAFF.—

(A) IN GENERAL.—The Secretary shall provide the Agency with a staff of analysts having appropriate expertise and experience to assist the Agency in discharging the responsibilities of the Agency under this section.

(B) PRIVATE SECTOR ANALYSTS.—Analysts under this subsection may include analysts from the private sector.

(C) SECURITY CLEARANCES.—Analysts under this subsection shall possess security clearances appropriate for their work under this section.

(4) DETAIL OF PERSONNEL.—

(A) IN GENERAL.—In order to assist the Agency in discharging the responsibilities of the Agency under this section, personnel of the Federal agencies described in subparagraph (B) may be detailed to the Agency for the performance of analytic functions and related duties.

(B) AGENCIES.—The Federal agencies described in this subparagraph are—

(i) the Department of State;

(ii) the Central Intelligence Agency;

(iii) the Federal Bureau of Investigation;

(iv) the National Security Agency;

(v) the National Geospatial-Intelligence Agency;

(vi) the Defense Intelligence Agency;

(vii) Sector-Specific Agencies; and

(viii) any other agency of the Federal Government that the President considers appropriate.

(C) INTERAGENCY AGREEMENTS.—The Secretary and the head of a Federal agency described in subparagraph (B) may enter into agreements for the purpose of detailing personnel under this paragraph.

(D) BASIS.—The detail of personnel under this paragraph may be on a reimbursable or non-reimbursable basis.

(f) COMPOSITION.—The Agency shall be composed of the following divisions:

(1) The Cybersecurity Division, headed by an Executive Assistant Director.

(2) The Infrastructure Security Division, headed by an Executive Assistant Director.

(3) The Emergency Communications Division under title XVIII, headed by an Executive Assistant Director.

(g) CO-LOCATION.—

(1) IN GENERAL.—To the maximum extent practicable, the Director shall examine the establishment of central locations in geographical regions with a significant Agency presence.

(2) COORDINATION.—When establishing the central locations described in paragraph (1), the Director shall coordinate with component heads and the Under Secretary for Management to co-locate or partner on any new real property leases, renewing any occupancy agreements for existing leases, or agreeing to extend or newly occupy any Federal space or new construction.

(h) PRIVACY.—

(1) IN GENERAL.—There shall be a Privacy Officer of the Agency with primary responsibility for privacy policy and compliance for the Agency.

(2) RESPONSIBILITIES.—The responsibilities of the Privacy Officer of the Agency shall include—

(A) assuring that the use of technologies by the Agency sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(B) assuring that personal information contained in systems of records of the Agency is handled in full compliance as specified in section 552a of title 5, United States Code (commonly known as the "Privacy Act of 1974");

(C) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Agency; and

(D) conducting a privacy impact assessment of proposed rules of the Agency on the privacy of personal information, including the type of personal information collected and the number of people affected.

(i) SAVINGS.—Nothing in this title may be construed as affecting in any manner the authority, existing on the day before the date of enactment of this title, of any other component of the Department or any other Federal department or agency, including the authority provided to the Sector Risk Management Agency specified

in section 61003(c) of division F of the Fixing America's Surface Transportation Act (6 U.S.C. 121 note; Public Law 114–94).

* * * * * * *

**SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE.**

(a) ESTABLISHMENT.—The Secretary shall establish within the Agency a Cybersecurity Advisory Committee (referred to in this section as the "Advisory Committee").

(b) DUTIES.—

(1) IN GENERAL.—The Advisory Committee shall advise, consult with, report to, and make recommendations to the Director, as appropriate, on the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency.

(2) RECOMMENDATIONS.—

(A) IN GENERAL.—The Advisory Committee shall develop, at the request of the Director, recommendations for improvements to advance the cybersecurity mission of the Agency and strengthen the cybersecurity of the United States.

(B) RECOMMENDATIONS OF SUBCOMMITTEES.—Recommendations agreed upon by subcommittees established under subsection (d) for any year shall be approved by the Advisory Committee before the Advisory Committee submits to the Director the annual report under paragraph (4) for that year.

(3) PERIODIC REPORTS.—The Advisory Committee shall periodically submit to the Director—

(A) reports on matters identified by the Director; and

(B) reports on other matters identified by a majority of the members of the Advisory Committee.

(4) ANNUAL REPORT.—

(A) IN GENERAL.—The Advisory Committee shall submit to the Director an annual report providing information on the activities, findings, and recommendations of the Advisory Committee, including its subcommittees, for the preceding year.

(B) PUBLICATION.—Not later than 180 days after the date on which the Director receives an annual report for a year under subparagraph (A), the Director shall publish a public version of the report describing the activities of the Advisory Committee and such related matters as would be informative to the public during that year, consistent with section 552(b) of title 5, United States Code.

(5) FEEDBACK.—Not later than 90 days after receiving any recommendation submitted by the Advisory Committee under paragraph (2), (3), or (4), the Director shall respond in writing to the Advisory Committee with feedback on the recommendation. Such a response shall include—

(A) with respect to any recommendation with which the Director concurs, an action plan to implement the recommendation; and

(B) with respect to any recommendation with which the Director does not concur, a justification for why the Director does not plan to implement the recommendation.

(6) CONGRESSIONAL NOTIFICATION.—Not less frequently than once per year after the date of enactment of this section, the Director shall provide to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security, the Committee on Energy and Commerce, and the Committee on Appropriations of the House of Representatives a briefing on feedback from the Advisory Committee.

(7) GOVERNANCE RULES.—The Director shall establish rules for the structure and governance of the Advisory Committee and all subcommittees established under subsection (d).

(c) MEMBERSHIP.—

(1) APPOINTMENT.—

(A) IN GENERAL.—Not later than 180 days after the date of enactment of the Cybersecurity Advisory Committee Authorization Act of 2020, the Director shall appoint the members of the Advisory Committee.

(B) COMPOSITION.—The membership of the Advisory Committee shall consist of not more than 35 individuals.

(C) REPRESENTATION.—

(i) IN GENERAL.—The membership of the Advisory Committee shall satisfy the following criteria:

(I) Consist of subject matter experts.

(II) Be geographically balanced.

(III) Include representatives of State, local, and Tribal governments and of a broad range of industries, which may include the following:

(aa) Defense.

(bb) Education.

(cc) Financial services and insurance.

(dd) Healthcare.

(ee) Manufacturing.

(ff) Media and entertainment.

(gg) Chemicals.

(hh) Retail.

(ii) Transportation.

(jj) Energy.

(kk) Information Technology.

(ll) Communications.

(mm) Other relevant fields identified by the Director.

(ii) PROHIBITION.—Not fewer than one member nor more than three members may represent any one category under clause (i)(III).

(iii) PUBLICATION OF MEMBERSHIP LIST.—The Advisory Committee shall publish its membership list on a publicly available website not less than once per fiscal year and shall update the membership list as changes occur.

(2) TERM OF OFFICE.—

(A) TERMS.—The term of each member of the Advisory Committee shall be two years, except that a member may continue to serve until a successor is appointed.

(B) REMOVAL.—The Director may review the participation of a member of the Advisory Committee and remove such member any time at the discretion of the Director.

(C) REAPPOINTMENT.—A member of the Advisory Committee may be reappointed for an unlimited number of terms.

(3) PROHIBITION ON COMPENSATION.—The members of the Advisory Committee may not receive pay or benefits from the United States Government by reason of their service on the Advisory Committee.

(4) MEETINGS.—

(A) IN GENERAL.—The Director shall require the Advisory Committee to meet not less frequently than semiannually, and may convene additional meetings as necessary.

(B) PUBLIC MEETINGS.—At least one of the meetings referred to in subparagraph (A) shall be open to the public.

(C) ATTENDANCE.—The Advisory Committee shall maintain a record of the persons present at each meeting.

(5) MEMBER ACCESS TO CLASSIFIED INFORMATION.—

(A) IN GENERAL.—Not later than 60 days after the date on which a member is first appointed to the Advisory Committee and before the member is granted access to any classified information, the Director shall determine, for the purposes of the Advisory Committee, if the member should be restricted from reviewing, discussing, or possessing classified information.

(B) ACCESS.—Access to classified materials shall be managed in accordance with Executive Order No. 13526 of December 29, 2009 (75 Fed. Reg. 707), or any subsequent corresponding Executive Order.

(C) PROTECTIONS.—A member of the Advisory Committee shall protect all classified information in accordance with the applicable requirements for the particular level of classification of such information.

(D) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to affect the security clearance of a member of the Advisory Committee or the authority of a Federal agency to provide a member of the Advisory Committee access to classified information.

(6) CHAIRPERSON.—The Advisory Committee shall select, from among the members of the Advisory Committee—

(A) a member to serve as chairperson of the Advisory Committee; and

(B) a member to serve as chairperson of each subcommittee of the Advisory Committee established under subsection (d).

(d) SUBCOMMITTEES.—

(1) IN GENERAL.—The Director shall establish subcommittees within the Advisory Committee to address cybersecurity issues, which may include the following:

(A) Information exchange.

(B) Critical infrastructure.

(C) Risk management.

(D) Public and private partnerships.

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

(2) MEETINGS AND REPORTING.—Each subcommittee shall meet not less frequently than semiannually, and submit to the Advisory Committee for inclusion in the annual report required under subsection (b)(4) information, including activities, findings, and recommendations, regarding subject matter considered by the subcommittee.

(3) SUBJECT MATTER EXPERTS.—The chair of the Advisory Committee shall appoint members to subcommittees and shall ensure that each member appointed to a subcommittee has subject matter expertise relevant to the subject matter of the subcommittee.

* * * * * * *

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

*(a) DEFINITION.—In this section, the term "software bill of materials" has the meaning given such term in the Minimum Elements for a Software Bill of Materials published by the Department of Commerce, or any superseding definition published by the Agency.*

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

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

*(2) perform the duties described in subsection (c).*

*(c) DUTIES OF THE DIRECTOR.—*

*(1) IN GENERAL.—The Director shall—*

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

*(B) support Federal efforts to strengthen the security of open source software;*

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

*(D) serve as a public point of contact regarding the security of open source software for non-Federal entities, including State, local, Tribal, and territorial partners, the private sector, international partners, and open source software communities; and*

*(E) support Federal and non-Federal supply chain security efforts by encouraging efforts to bolster open source software security, such as—*

*(i) assisting in coordinated vulnerability disclosures in open source software components pursuant to section 2209(n); and*

*(ii) supporting the activities of the Federal Acquisition Security Council.*

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

*(A) FRAMEWORK.—Not later than one year after the date of the enactment of this section, the Director shall publicly publish a framework, incorporating government, private sector, and open source software community frameworks and best practices, including those published by the National Institute of Standards and Technology, for assessing*

*the risk of open source software components, including direct and indirect open source software dependencies, which shall incorporate, at a minimum, the following with respect to a given open source software component:*

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

*(ii) The security practices of development, build, and release processes, such as the use of multi-factor authentication by maintainers and cryptographic signing of releases.*

*(iii) The number and severity of publicly known, unpatched vulnerabilities.*

*(iv) The breadth of deployment.*

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

*(vi) The health and sustainability of the open source software community, including, where applicable, the level of current and historical investment and maintenance in such component, such as the number and activity of individual maintainers.*

*(B) UPDATING FRAMEWORK.—Not less frequently than annually after the date on which the framework is published under subparagraph (A), the Director shall—*

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

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

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

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

*(ii) The open source software community.*

*(D) USABILITY.—The Director shall ensure, to the greatest extent practicable, that the framework described in subparagraph (A) is usable by the open source software community, including through the consultation required under subparagraph (C).*

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

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

*(I) software bills of material that are, at the time of the assessment, made available to the Agency or are otherwise accessible via the internet;*

*(II) software inventories, available to the Director at the time of the assessment, from the Continuous Diagnostics and Mitigation program of the Agency; and*

*(III) other publicly available information regarding open source software components; and*

*(ii) develop, in consultation with the Federal agency at which an open source software component is deployed, one or more ranked lists of components described in clause (i) based on such assessment, such as ranked by the criticality, level of risk, or usage of the components, or a combination thereof.*

*(F) AUTOMATION.—The Director shall, to the greatest extent practicable, automate the assessment performed pursuant to subparagraph (E).*

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

*(H) SHARING.—*

*(i) RESULTS.—The Director, to the greatest extent practicable, and taking into account the sensitivity of the information contained in the assessment performed pursuant to subparagraph (E), shall facilitate the sharing of the results of each assessment under subparagraph (E)(i) with appropriate Federal and non-Federal entities working to support the security of open source software, including by offering means for appropriate Federal and non-Federal entities to download the assessment in an automated manner.*

*(ii) DATASETS.—The Director may publicly publish, as appropriate, any datasets or versions of the datasets developed or consolidated as a result of an assessment under subparagraph (E)(i).*

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

*(i) STUDY.—Not later than two years after the publication of the framework under subparagraph (A), the Director shall conduct a study regarding the feasibility of the Director conducting the assessment under subparagraph (E) for critical infrastructure entities.*

*(ii) PILOT.—*

*(I) IN GENERAL.—If the Director determines that the assessment described in clause (i) is feasible, the Director may conduct a pilot assessment on a voluntary basis with one or more critical infrastructure sectors, in coordination with the Sector Risk Management Agency and the sector coordinating council of each participating sector.*

*(II) TERMINATION.—If the Director proceeds with the pilot assessment described in subclause (I), such pilot assessment shall terminate not later*

*than two years after the date on which the Director begins such pilot assessment.*

*(iii) REPORTS.—*

*(I) STUDY.—Not later than 180 days after the date on which the Director completes the study conducted under clause (i), the Director shall submit to the appropriate congressional committees a report that—*

*(aa) summarizes the study;*

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

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

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

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

*(II) PILOT.—If the Director proceeds with the pilot assessment described in clause (ii), not later than one year after the date on which the Director begins such pilot assessment, the Director shall submit to the appropriate congressional committees a report that includes the following:*

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

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

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

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

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

*(4) REPORTS.—*

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

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

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

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

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

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

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

*(B) PUBLIC REPORT.—Not later than 30 days after the date on which the Director submits each report required under subparagraph (A), the Director shall make a version of each such report publicly available on the website of the Agency.*

* * * * * * *

○