Calendar No. 382

118TH CONGRESS *2d Session*	SENATE	REPORT 118–171

NATIONAL CYBERSECURITY AWARENESS ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 1835

TO REQUIRE THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY OF THE DEPARTMENT OF HOMELAND SECURITY TO DEVELOP A CAMPAIGN PROGRAM TO RAISE AWARENESS REGARDING THE IMPORTANCE OF CYBERSECURITY IN THE UNITED STATES

MAY 9, 2024.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
49–010 WASHINGTON : 2024

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
JON OSSOFF, Georgia	RICK SCOTT, Florida
RICHARD BLUMENTHAL, Connecticut	JOSH HAWLEY, Missouri
LAPHONZA R. BUTLER, California	ROGER MARSHALL, Kansas

DAVID M. WEINBERG, *Staff Director*
ALAN S. KAHN, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
EMILY A. FERGUSON, *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. 382

118TH CONGRESS
2d Session

SENATE

REPORT
118–171

NATIONAL CYBERSECURITY AWARENESS ACT

MAY 9, 2024.—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. 1835]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 1835) to require the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security to develop a campaign program to raise awareness regarding the importance of cybersecurity in the United States, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 1835, the *National Cybersecurity Awareness Act*, directs the Cybersecurity and Infrastructure Security Agency (CISA) to lead federal efforts in promoting cybersecurity education and awareness. Specifically, the bill directs CISA to develop a campaign program that informs the public of cyber hygiene best practices, including how to prevent cyberattacks and mitigate general cybersecurity risks. CISA would coordinate with other federal agencies and departments to promote cybersecurity-related awareness activities

and to ensure the government communicates accurate and timely information. The awareness campaign would be conducted in consultation with private sector entities, state, local, tribal, and territorial (SLTT) governments, and civil society to promote cybersecurity awareness, including how to effectively communicate awareness. The bill also requires that low-income and rural communities, small and mid-sized businesses, and other historically unrepresented institutions receive specific outreach. Finally, the bill requires that awareness campaign resources be made publicly available online and regularly updated, and that CISA report to Congress on the Agency's awareness campaign strategy and the efficacy of their efforts.

II. Background and the Need for Legislation

The presence of internet-connected devices in modern society has created opportunities for both constant connection and for malicious actors to engage in illicit activities.[1] It has thus become increasingly important for the U.S. to have a cybersecurity posture that includes the cooperation of government and industry to keep the public fully informed of how to stay safe in cyberspace.[2]

Congress and the President underscored this in establishing Cybersecurity Awareness Month in 2004.[3] Each October thereafter, government and industry have led collaborative efforts to raise cybersecurity awareness nationally. This Committee has passed several pieces of bipartisan legislation aimed at enhancing the government's ability to provide cybersecurity assistance and outreach, including the *K–12 Cybersecurity Act of 2021*, which enhances CISA's cyber assistance efforts to K–12 schools, and the *State and Local Government Cybersecurity Act of 2021*, which fosters greater collaboration between the federal government and nonfederal government entities.[4] The Senate has also passed multiple Senate Resolutions recognizing the importance of Cybersecurity Awareness Month.[5]

CISA has established and enhanced cybersecurity assistance and outreach to the public as a part of its mission to strengthen the United States' resilience against cyberattacks.[6] Even with these and other federal efforts, securing cyberspace remains challenging given the ability of malicious actors to operate worldwide, the varying levels of interconnectedness between cyberspace and physical

---

[1] Federal Bureau of Investigation, *Internet Crime Report 2023* (Mar. 2024) (www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf).

[2] Cybersecurity & Infrastructure Security Agency, *Cybersecurity Best Practices* (accessed May 3, 2024) (www.cisa.gov/topics/cybersecurity-best-practices).

[3] Cybersecurity & Infrastructure Security Agency, *Cybersecurity Awareness Month* (accessed June 2, 2023) (www.cisa.gov/cybersecurity-awareness-month).

[4] K–12 Cybersecurity Act of 2021, Pub. L. No. 117–47; State and Local Government Cybersecurity Act of 2021, Pub. L. No. 117–150.

[5] S. Res. 410. 117th Cong. 1st Sess. (2021), S. Res. 345. 116th Cong. 1st Sess. (2019), S. Res. 306. 112th Cong. 1st Sess. (2011), S. Res. 285. 111th Con. 1st Sess. (2009), and S. Res. 697. 110th Con. 2nd Sess. (2008).

[6] Cybersecurity and Infrastructure Security Agency, *Cybersecurity Best Practices* (www.cisa.gov/topics/cybersecurity-best-practices); Cybersecurity and Infrastructure Security Agency, Free Cybersecurity Services and Tools (www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools); Cybersecurity and Infrastructure Security Agency, *CISA Analysis: Fiscal Year 2022 Risk and Vulnerability Assessments* (June 2023) (www.cisa.gov/sites/default/files/2023-07/FY22-RVA-Analysis%20-%20Final_508c.pdf).

systems, and difficulties in reducing vulnerabilities in complex cyber networks.[7]

As such, cyber threats such as personal data breaches, phishing campaigns and malware have increased in recent years. Americans lost an estimated $10.3 billion to cybercrime in 2022, an increase from $6.9 billion in 2021.[8] The Federal Bureau of Investigation has received over 651,800 complaints of cybercrime every year on average for the past five years.[9] Globally, cybercrime rose 600% during the height of the COVID–19 pandemic.[10]

To continue to address these evolving threats, raising cybersecurity awareness cannot be a once-a-year activity. This bill addresses the need for more continuous outreach by codifying national cybersecurity efforts led by CISA and strengthening the partnerships between the government, public entities, and private organizations. Through these partnerships, CISA will promote cost-effective cybersecurity strategies informed by cyber threat research data, leading to more resilient organizational postures. By requiring an annual report to Congress on the effectiveness of the awareness campaign program, this bill enhances the oversight of the federal government's existing cybersecurity outreach efforts.

III. LEGISLATIVE HISTORY

Senator Gary Peters (D–MI) introduced S. 1835, the *National Cybersecurity Awareness Act*, on June 6, 2023, with original cosponsor Senator Bill Cassidy (R–LA). The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 1835 at a business meeting on June 14, 2023. At the business meeting, Senator Peters offered an amendment in the nature of a substitute to add a requirement that the Director of CISA coordinate with appropriate federal agencies in the establishment of the awareness program, to reference existing National Institute of Standards and Technology Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things Products, and to make technical edits. The Committee adopted the Peters substitute amendment by unanimous consent with Senator Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Blumenthal, Paul, Lankford, Romney, Scott, Hawley, and Marshall present.

The bill, as amended by the Peters substitute amendment, was ordered reported favorably by a roll call vote of 10 yeas and 2 nays, with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Blumenthal, Lankford, Romney, and Hawley voting in the affirmative, and Senators Paul and Scott 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.

---

[7] Cybersecurity and Infrastructure Security Agency, *Cybersecurity Best Practices* (www.cisa.gov/topics/cybersecurity-best-practices).

[8] Federal Bureau of Investigation, *Internet Crime Report 2022* (Mar. 2023) (www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf?ref=marketsplash.com).

[9] *Id*.

[10] *UN Warns Cybercrime on Rise During Pandemic*, Associated Press (May 23, 2020) (apnews.com/article/europe-united-nations-brazil-south-korea-cybercrime-6ba6af57fd96e25334d8a06fcf999e7f).

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

Section 1. Short title

This section designates the name of the bill as the "National Cybersecurity Awareness Act."

Section 2. Findings

This section outlines Congressional findings that: (1) the presence of ubiquitous internet-connected devices in the lives of American citizens has created opportunities for constant connection and modernization; a connected society is subject to cybersecurity threats; (2) connected critical infrastructure is subject to cybersecurity threats that can compromise fundamental economic health, and safety functions; the United States government plays an important role in safeguarding the nation from malicious cyber activity; (3) a citizenry that is knowledgeable regarding cybersecurity is critical to building a robust cybersecurity posture and reducing the threat of cyber attackers; and (4) that supporting national cybersecurity awareness must be a sustained, constant effort.

Section 3. Cybersecurity awareness

Subsection (a) amends Subtitle A of title XXII of the Homeland Security Act of 2002 by adding a new section 220F titled "Cybersecurity Awareness Campaigns."

Section 220F, subsection (a) defines the term "Campaign Program" to mean the campaign program established under subsection (b).

Section 220F, subsection (b)(1) requires the Director of CISA to establish a program for planning and coordinating cybersecurity awareness campaigns no later than 90 days after the enactment of the bill.

Section 220F, subsection (b)(2)(A) requires the Director of CISA to inform non-federal entities of voluntary cyber hygiene best practices, including information on how to prevent cyberattacks and mitigate security risks.

Section 220F, subsection (b)(2)(B) requires the Director of CISA to consult with private sector entities, state, local, tribal, and territorial governments, academia, and civil society to promote cyber hygiene best practices, including by focusing on tactics that are cost effective and result in significant cybersecurity improvement, such as: maintaining strong passwords, enabling multi-factor authentication, regularly installing software updates, using caution with email attachments and links, and other cyber hygienic considerations. In consultation with these entities, the Director of CISA must also: promote awareness of cybersecurity risks and mitigation with respect to malicious applications on internet-connected devices; help consumers identify products that are designed to support user and product security; coordinate with other federal agencies and departments to promote relevant cybersecurity-related awareness activities and ensure the federal government is coordinated in communicating accurate and timely cybersecurity information; and expand nontraditional outreach mechanisms to ensure that entities including low-income and rural communities, small and medium sized businesses and institutions, and state, local,

tribal, and territorial partners receive cybersecurity awareness outreach.

Section 220F, subsection (b)(3) requires the Director of CISA, in consultation with the heads of appropriate federal agencies, to submit a report regarding the Campaign Program to the appropriate congressional committees no later than 180 days after the enactment of the bill and annually thereafter. Each report shall include a summary CISA activities that support promoting cybersecurity awareness under the Campaign Program, an assessment of the effectiveness of techniques and methods used to promote cybersecurity awareness, and recommendations on how to best promote cybersecurity awareness nationally.

Section 220F, subsection (c) requires the Director of CISA, no later than 180 days after the enactment of the bill, to develop and maintain a central repository for the resources, tools, and public communications of the Agency that promote cybersecurity awareness. These resources must be publicly available online and regularly updated to ensure the public has access to relevant and timely cybersecurity awareness information.

Subsection (b) amends the formatting of Section 2202(c) of the Homeland Security Act of 2002 and inserts a clause after paragraph (13) that states CISA will lead and coordinate federal efforts to promote national cybersecurity awareness.

Subsection (c) amends the table of contents located in section 1(b) of the Homeland Security Act of 2002 by adding Section 220F.

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

S. 1835, National Cybersecurity Awareness Act
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on June 14, 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	*	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

* = between zero and $500,000.

S. 1835 would require the Cybersecurity and Infrastructure Security Agency (CISA) to raise public awareness about cyber threats and safe computing practices. The bill also would require the agency to report annually to the Congress on the effectiveness of its efforts.

CISA currently promotes safe online behavior through the Cybersecurity Awareness Program. S. 1835 would codify those responsibilities and would not impose any new operating requirements on the agency. CBO estimates that implementing S. 1835 would cost less than $500,000 over the 2023–2028 period to prepare the required reports; any spending would be subject to the availability of appropriated funds.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Christina Hawley Anthony, Deputy Director of Budget Analysis.

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

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) * * *
(b) * * *
(c) * * *
(1) * * *

* * * * * * *

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

(14) lead and coordinate Federal efforts to promote national cybersecurity awareness; and

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

* * * * * * *

SEC. 2220F. CYBERSECURITY AWARENESS CAMPAIGNS.

(a) DEFINITION.—In this section, the term 'Campaign Program' means the campaign program established under subsection (b)(1).

(b) AWARENESS CAMPAIGN PROGRAM.—

(1) IN GENERAL.—Not later than 90 days after the date of enactment of the National Cybersecurity Awareness Act, the Director, in coordination with appropriate Federal agencies, shall establish a program for planning and coordinating Federal cybersecurity awareness campaigns.

(2) ACTIVITIES.—In carrying out the Campaign Program, the Director shall—

(A) inform non-Federal entities of voluntary cyber hygiene best practices, including information on how to—

(i) prevent cyberattacks; and

(ii) mitigate cybersecurity risks; and

(B) consult with private sector entities, State, local, Tribal, and territorial governments, academia, nonprofit organizations, and civil society—

(i) to promote cyber hygiene best practices and the importance of cyber skills, including by focusing on tactics that are cost effective and result in significant cybersecurity improvement, such as—

(I) maintaining strong passwords and the use of password managers;

(II) enabling multi-factor authentication, including phishing-resistant multi-factor authentication;

(III) regularly installing software updates;

(IV) using caution with email attachments and website links; and

(V) other cyber hygienic considerations, as appropriate;

(ii) to promote awareness of cybersecurity risks and mitigation with respect to malicious applications on internet-connected devices, including applications to control those devices or use devices for unauthorized surveillance of users;

(iii) to help consumers identify products that are designed to support user and product security, such as products designed using the Secure-by-Design and Secure-by-Default principles of the Agency or the Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products of the National Institute of Standards and Technology, published February 4, 2022 (or any subsequent version);

(iv) to coordinate with other Federal agencies, as determined appropriate by the Director, to—

(I) develop and promote relevant cybersecurity-related and cyber skills-related awareness activities and resources; and

(II) ensure the Federal Government is coordinated in communicating accurate and timely cybersecurity information;

(v) to expand nontraditional outreach mechanisms to ensure that entities, including low-income and rural communities, small and medium sized businesses and institutions, and State, local, Tribal, and territorial partners, receive cybersecurity awareness outreach in an equitable manner; and

(vi) to encourage participation in cyber workforce development ecosystems and to expand adoption of best practices to grow the national cyber workforce.

(3) REPORTING.—

(A) IN GENERAL.—Not later than 180 days after the date of enactment of the National Cybersecurity Awareness Act, and annually thereafter, the Director, in consultation with the heads of appropriate Federal agencies, shall submit to the appropriate congressional committees a report regarding the Campaign Program.

(B) CONTENTS.—Each report submitted pursuant to subparagraph (A) shall include—

(i) a summary of the activities of the Agency that support promoting cybersecurity awareness under the

Campaign Program, including consultations made under paragraph (2)(B);

(ii) an assessment of the effectiveness of techniques and methods used to promote national cybersecurity awareness under the Campaign Program; and

(iii) recommendations on how to best promote cybersecurity awareness nationally.

(c) CYBERSECURITY CAMPAIGN RESOURCES.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of the National Cybersecurity Awareness Act, the Director shall develop and maintain a repository for the resources, tools, and public communications of the Agency that promote cybersecurity awareness.

(2) REQUIREMENTS.—The resources described in paragraph (1) shall be—

(A) made publicly available online; and

(B) regularly updated to ensure the public has access to relevant and timely cybersecurity awareness information.

* * * * * * *

○