AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 382

118TH CONGRESS
2D SESSION

S. 1835

[Report No. 118–171]

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.

IN THE SENATE OF THE UNITED STATES

JUNE 6, 2023

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

MAY 9, 2024

Reported by Mr. PETERS, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

A BILL

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''National Cybersecurity Awareness Act''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) The presence of ubiquitous internet-connected devices in the everyday lives of citizens of the United States has created opportunities for constant connection and modernization.

(2) A connected society is subject to cybersecurity threats that can compromise even the most personal and sensitive of information.

(3) Connected critical infrastructure is subject to cybersecurity threats that can compromise fundamental economic and health and safety functions.

(4) The Government of the United States plays an important role in safeguarding the nation from malicious cyber activity.

(5) A citizenry that is knowledgeable regarding cybersecurity is critical to building a robust cybersecurity posture and reducing the threat of cyber attackers stealing sensitive information and causing public harm.

(6) While Cybersecurity Awareness Month is critical to supporting national cybersecurity aware-

ness, it cannot be a once-a-year activity and must be a sustained, constant effort.

SEC. 3. CYBERSECURITY AWARENESS.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following:

"SEC. 2220F. CYBERSECURITY AWARENESS CAMPAIGNS.

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

"(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 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, and civil society—

"(i) to promote cyber hygiene best practices, 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;

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

“(I) promote relevant cybersecurity-related awareness activities; and

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

“(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.

“(3) REPORTING.—

“(A) IN GENERAL.—Not later than 180 days after the date of enactment of the Na-

tional Cybersecurity Awareness Act, and annually thereafter, the Director shall, in consultation with the heads of appropriate Federal agencies, 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 central 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.''.

(b) RESPONSIBILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—Section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)) is amended—

(1) in paragraph (13), by striking ''; and'' and inserting a semicolon;

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

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

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

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by inserting after the item relating to section 2220E the following:

''Sec. 2220F. Cybersecurity awareness campaigns''.

SECTION 1. SHORT TITLE.

This Act may be cited as the "National Cybersecurity Awareness Act".

SEC. 2. FINDINGS.

Congress finds the following:

(1) The presence of ubiquitous internet-connected devices in the everyday lives of citizens of the United States has created opportunities for constant connection and modernization.

(2) A connected society is subject to cybersecurity threats that can compromise even the most personal and sensitive of information.

(3) Connected critical infrastructure is subject to cybersecurity threats that can compromise fundamental economic, health, and safety functions.

(4) The Government of the United States plays an important role in safeguarding the nation from malicious cyber activity.

(5) A citizenry that is knowledgeable regarding cybersecurity is critical to building a robust cybersecurity posture and reducing the threat of cyber attackers stealing sensitive information and causing public harm.

(6) While Cybersecurity Awareness Month is critical to supporting national cybersecurity awareness, it cannot be a once-a-year activity, and there

must be a sustained, constant effort to raise awareness about cyber hygiene, encourage individuals in the United States to learn cyber skills, and communicate the ways that cyber skills and careers in cyber advance individual and societal security, privacy, safety, and well-being.

SEC. 3. CYBERSECURITY AWARENESS.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following:

"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.".

(b) RESPONSIBILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—Section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)) is amended—

(1) in paragraph (13), by striking "; and" and inserting a semicolon;

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

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

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

(c) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by inserting after the item relating to section 2220E the following:

"Sec. 2220F. Cybersecurity awareness campaigns.".

Calendar No. 382

118TH CONGRESS
2D SESSION

S. 1835

[Report No. 118–171]

A BILL

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

Reported with an amendment