

118TH CONGRESS
1ST SESSION

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.

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

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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “National Cybersecurity
5 Awareness Act”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

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

5 (2) A connected society is subject to cybersecu-
6 rity threats that can compromise even the most per-
7 sonal and sensitive of information.

8 (3) Connected critical infrastructure is subject
9 to cybersecurity threats that can compromise funda-
10 mental economic and health and safety functions.

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

14 (5) A citizenry that is knowledgeable regarding
15 cybersecurity is critical to building a robust cyberse-
16 curity posture and reducing the threat of cyber
17 attackers stealing sensitive information and causing
18 public harm.

19 (6) While Cybersecurity Awareness Month is
20 critical to supporting national cybersecurity aware-
21 ness, it cannot be a once-a-year activity and must be
22 a sustained, constant effort.

1 **SEC. 3. CYBERSECURITY AWARENESS.**

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

5 **“SEC. 2220F. CYBERSECURITY AWARENESS CAMPAIGNS.**

6 “(a) DEFINITION.—In this section, the term ‘Cam-
7 paign Program’ means the campaign program established
8 under subsection (b).

9 “(b) AWARENESS CAMPAIGN PROGRAM.—

10 “(1) IN GENERAL.—Not later than 90 days
11 after the date of enactment of the National Cyberse-
12 curity Awareness Act, the Director shall establish a
13 program for planning and coordinating Federal cy-
14 bersecurity awareness campaigns.

15 “(2) ACTIVITIES.—In carrying out the Cam-
16 paign Program, the Director shall—

17 “(A) inform non-Federal entities of vol-
18 untary cyber hygiene best practices, including
19 information on how to—

20 “(i) prevent cyberattacks; and

21 “(ii) mitigate cybersecurity risks; and

22 “(B) consult with private sector entities,
23 State, local, Tribal, and territorial governments,
24 academia, and civil society—

25 “(i) to promote cyber hygiene best
26 practices, including by focusing on tactics

1 that are cost effective and result in signifi-
2 cant cybersecurity improvement, such as—

3 “(I) maintaining strong pass-
4 words and the use of password man-
5 agers;

6 “(II) enabling multi-factor au-
7 thentication, including phishing-resist-
8 ant multi-factor authentication;

9 “(III) regularly installing soft-
10 ware updates;

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

13 “(V) other cyber hygienic consid-
14 erations, as appropriate;

15 “(ii) to promote awareness of cyberse-
16 curity risks and mitigation with respect to
17 malicious applications on internet-con-
18 nected devices, including applications to
19 control those devices or use devices for un-
20 authorized surveillance of users;

21 “(iii) to help consumers identify prod-
22 ucts that are designed to support user and
23 product security, such as products de-
24 signed using the Secure-by-Design and Se-
25 cure-by-Default principles of the Agency;

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

4 “(I) promote relevant cybersecu-
5 rity-related awareness activities; and

6 “(II) ensure the Federal Govern-
7 ment is coordinated in communicating
8 accurate and timely cybersecurity in-
9 formation; and

10 “(v) to expand nontraditional out-
11 reach mechanisms to ensure that entities
12 including low-income and rural commu-
13 nities, small and medium sized businesses
14 and institutions, and State, local, Tribal,
15 and territorial partners receive cybersecu-
16 rity awareness outreach in an equitable
17 manner.

18 “(3) REPORTING.—

19 “(A) IN GENERAL.—Not later than 180
20 days after the date of enactment of the Na-
21 tional Cybersecurity Awareness Act, and annu-
22 ally thereafter, the Director shall, in consulta-
23 tion with the heads of appropriate Federal
24 agencies, submit to the appropriate congres-

1 sional committees a report regarding the Cam-
2 paign Program.

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

5 “(i) a summary of the activities of the
6 Agency that support promoting cybersecu-
7 rity awareness under the Campaign Pro-
8 gram, including consultations made under
9 paragraph (2)(B);

10 “(ii) an assessment of the effective-
11 ness of techniques and methods used to
12 promote national cybersecurity awareness
13 under the Campaign Program; and

14 “(iii) recommendations on how to best
15 promote cybersecurity awareness nation-
16 ally.

17 “(c) CYBERSECURITY CAMPAIGN RESOURCES.—

18 “(1) IN GENERAL.—Not later than 180 days
19 after the date of enactment of the National Cyberse-
20 curity Awareness Act, the Director shall develop and
21 maintain a central repository for the resources,
22 tools, and public communications of the Agency that
23 promote cybersecurity awareness.

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

1 “(A) made publicly available online; and

2 “(B) regularly updated to ensure the pub-
3 lic has access to relevant and timely cybersecu-
4 rity awareness information.”.

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

9 (1) in paragraph (13), by striking “; and” and
10 inserting a semicolon;

11 (2) by redesignating paragraph (14) as para-
12 graph (15); and

13 (3) by inserting after paragraph (13) the fol-
14 lowing:

15 “(14) lead and coordinate Federal efforts to
16 promote national cybersecurity awareness; and”.

17 (c) CLERICAL AMENDMENT.—The table of contents
18 in section 1(b) of the Homeland Security Act of 2002
19 (Public Law 107–296; 116 Stat. 2135) is amended by in-
20 serting after the item relating to section 2220E the fol-
21 lowing:

“Sec. 2220F. Cybersecurity awareness campaigns”.

○