

# Calendar No. 382

118<sup>TH</sup> CONGRESS  
2<sup>D</sup> 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 *italie*]

---

## 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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “National Cybersecurity  
3 Awareness Act”.

4 **SEC. 2. FINDINGS.**

5 Congress finds the following:

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

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

13 (3) Connected critical infrastructure is subject  
14 to cybersecurity threats that can compromise funda-  
15 mental economic and health and safety functions.

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

19 (5) A citizenry that is knowledgeable regarding  
20 cybersecurity is critical to building a robust cyberse-  
21 curity posture and reducing the threat of cyber  
22 attackers stealing sensitive information and causing  
23 public harm.

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

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

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

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

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

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

11           “(b) **AWARENESS CAMPAIGN PROGRAM.**—

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

17                   “(2) **ACTIVITIES.**—In carrying out the Cam-  
18 paign Program, the Director shall—

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

22                                   “(i) prevent cyberattacks; and

23                                   “(ii) mitigate cybersecurity risks; and

1           “(B) consult with private sector entities,  
2           State, local, Tribal, and territorial governments,  
3           academia, and civil society—

4                   “(i) to promote cyber hygiene best  
5                   practices, including by focusing on tactics  
6                   that are most effective and result in signifi-  
7                   cant cybersecurity improvement, such as—

8                           “(I) maintaining strong pass-  
9                           words and the use of password man-  
10                           agers;

11                           “(II) enabling multi-factor au-  
12                           thentication, including phishing-resist-  
13                           ant multi-factor authentication;

14                           “(III) regularly installing soft-  
15                           ware updates;

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

18                           “(V) other cyber hygienic consid-  
19                           erations, as appropriate;

20                   “(ii) to promote awareness of cyberse-  
21                   curity risks and mitigation with respect to  
22                   malicious applications on internet-con-  
23                   nected devices, including applications to  
24                   control those devices or use devices for un-  
25                   authorized surveillance of users;

1           ~~“(iii) to help consumers identify prod-~~  
2           ~~ucts that are designed to support user and~~  
3           ~~product security, such as products de-~~  
4           ~~signed using the Secure-by-Design and Se-~~  
5           ~~ecure-by-Default principles of the Agency;~~

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

9                   ~~“(I) promote relevant cybersecu-~~  
10                   ~~rity-related awareness activities; and~~

11                   ~~“(II) ensure the Federal Govern-~~  
12                   ~~ment is coordinated in communicating~~  
13                   ~~accurate and timely cybersecurity in-~~  
14                   ~~formation; and~~

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

23           ~~“(3) REPORTING.—~~

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

1           tional Cybersecurity Awareness Act, and annu-  
2           ally thereafter, the Director shall, in consulta-  
3           tion with the heads of appropriate Federal  
4           agencies, submit to the appropriate congress-  
5           sional committees a report regarding the Cam-  
6           paign Program.

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

9                   “(i) a summary of the activities of the  
10                  Agency that support promoting cybersecu-  
11                  rity awareness under the Campaign Pro-  
12                  gram, including consultations made under  
13                  paragraph (2)(B);

14                  “(ii) an assessment of the effective-  
15                  ness of techniques and methods used to  
16                  promote national cybersecurity awareness  
17                  under the Campaign Program; and

18                  “(iii) recommendations on how to best  
19                  promote cybersecurity awareness nation-  
20                  ally.

21           “(c) CYBERSECURITY CAMPAIGN RESOURCES.—

22                   “(1) IN GENERAL.—Not later than 180 days  
23                  after the date of enactment of the National Cyberse-  
24                  curity Awareness Act, the Director shall develop and  
25                  maintain a central repository for the resources;

1 tools, and public communications of the Agency that  
 2 promote cybersecurity awareness.

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

5 “(A) made publicly available online; and

6 “(B) regularly updated to ensure the pub-  
 7 lic has access to relevant and timely cybersecu-  
 8 rity awareness information.”.

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

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

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

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

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

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

“Sec. 2220F. Cybersecurity awareness campaigns”.

1 **SECTION 1. SHORT TITLE.**

2 *This Act may be cited as the “National Cybersecurity*  
3 *Awareness Act”.*

4 **SEC. 2. FINDINGS.**

5 *Congress finds the following:*

6 *(1) The presence of ubiquitous internet-connected*  
7 *devices in the everyday lives of citizens of the United*  
8 *States has created opportunities for constant connec-*  
9 *tion and modernization.*

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

13 *(3) Connected critical infrastructure is subject to*  
14 *cybersecurity threats that can compromise funda-*  
15 *mental economic, health, and safety functions.*

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

19 *(5) A citizenry that is knowledgeable regarding*  
20 *cybersecurity is critical to building a robust cyberse-*  
21 *curity posture and reducing the threat of cyber*  
22 *attackers stealing sensitive information and causing*  
23 *public harm.*

24 *(6) While Cybersecurity Awareness Month is*  
25 *critical to supporting national cybersecurity aware-*  
26 *ness, it cannot be a once-a-year activity, and there*



1       *must be a sustained, constant effort to raise aware-*  
2       *ness about cyber hygiene, encourage individuals in*  
3       *the United States to learn cyber skills, and commu-*  
4       *nicate the ways that cyber skills and careers in cyber*  
5       *advance individual and societal security, privacy,*  
6       *safety, and well-being.*

7       **SEC. 3. CYBERSECURITY AWARENESS.**

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

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

12      *“(a) DEFINITION.—In this section, the term ‘Cam-*  
13      *paign Program’ means the campaign program established*  
14      *under subsection (b)(1).*

15      *“(b) AWARENESS CAMPAIGN PROGRAM.—*

16              *“(1) IN GENERAL.—Not later than 90 days after*  
17              *the date of enactment of the National Cybersecurity*  
18              *Awareness Act, the Director, in coordination with ap-*  
19              *propriate Federal agencies, shall establish a program*  
20              *for planning and coordinating Federal cybersecurity*  
21              *awareness campaigns.*

22              *“(2) ACTIVITIES.—In carrying out the Cam-*  
23              *paign Program, the Director shall—*

1           “(A) inform non-Federal entities of vol-  
2           untary cyber hygiene best practices, including  
3           information on how to—

4                   “(i) prevent cyberattacks; and

5                   “(ii) mitigate cybersecurity risks; and

6           “(B) consult with private sector entities,  
7           State, local, Tribal, and territorial governments,  
8           academia, nonprofit organizations, and civil so-  
9           ciety—

10                   “(i) to promote cyber hygiene best  
11           practices and the importance of cyber skills,  
12           including by focusing on tactics that are  
13           cost effective and result in significant cyber-  
14           security improvement, such as—

15                   “(I) maintaining strong pass-  
16           words and the use of password man-  
17           agers;

18                   “(II) enabling multi-factor au-  
19           thentication, including phishing-resist-  
20           ant multi-factor authentication;

21                   “(III) regularly installing soft-  
22           ware updates;

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

1                   “(V) *other cyber hygienic consid-*  
2                   *erations, as appropriate;*

3                   “(ii) *to promote awareness of cyberse-*  
4                   *curity risks and mitigation with respect to*  
5                   *malicious applications on internet-con-*  
6                   *ected devices, including applications to*  
7                   *control those devices or use devices for un-*  
8                   *authorized surveillance of users;*

9                   “(iii) *to help consumers identify prod-*  
10                  *ucts that are designed to support user and*  
11                  *product security, such as products designed*  
12                  *using the Secure-by-Design and Secure-by-*  
13                  *Default principles of the Agency or the Rec-*  
14                  *ommended Criteria for Cybersecurity Label-*  
15                  *ing for Consumer Internet of Things (IoT)*  
16                  *Products of the National Institute of Stand-*  
17                  *ards and Technology, published February 4,*  
18                  *2022 (or any subsequent version);*

19                  “(iv) *to coordinate with other Federal*  
20                  *agencies, as determined appropriate by the*  
21                  *Director, to—*

22                  “(I) *develop and promote relevant*  
23                  *cybersecurity-related and cyber skills-*  
24                  *related awareness activities and re-*  
25                  *sources; and*

1                   “(II) ensure the Federal Govern-  
2                   ment is coordinated in communicating  
3                   accurate and timely cybersecurity in-  
4                   formation;

5                   “(v) to expand nontraditional outreach  
6                   mechanisms to ensure that entities, includ-  
7                   ing low-income and rural communities,  
8                   small and medium sized businesses and in-  
9                   stitutions, and State, local, Tribal, and ter-  
10                  ritorial partners, receive cybersecurity  
11                  awareness outreach in an equitable manner;  
12                  and

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

17                  “(3) REPORTING.—

18                  “(A) IN GENERAL.—Not later than 180  
19                  days after the date of enactment of the National  
20                  Cybersecurity Awareness Act, and annually  
21                  thereafter, the Director, in consultation with the  
22                  heads of appropriate Federal agencies, shall sub-  
23                  mit to the appropriate congressional committees  
24                  a report regarding the Campaign Program.

1           “(B) *CONTENTS.*—*Each report submitted*  
2           *pursuant to subparagraph (A) shall include—*

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

8                   “(ii) *an assessment of the effectiveness*  
9                   *of techniques and methods used to promote*  
10                   *national cybersecurity awareness under the*  
11                   *Campaign Program; and*

12                   “(iii) *recommendations on how to best*  
13                   *promote cybersecurity awareness nationally.*

14           “(c) *CYBERSECURITY CAMPAIGN RESOURCES.*—

15                   “(1) *IN GENERAL.*—*Not later than 180 days*  
16                   *after the date of enactment of the National Cybersecu-*  
17                   *rity Awareness Act, the Director shall develop and*  
18                   *maintain a repository for the resources, tools, and*  
19                   *public communications of the Agency that promote*  
20                   *cybersecurity awareness.*

21                   “(2) *REQUIREMENTS.*—*The resources described*  
22                   *in paragraph (1) shall be—*

23                   “(A) *made publicly available online; and*

1                   “(B) regularly updated to ensure the public  
2                   has access to relevant and timely cybersecurity  
3                   awareness information.”.

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

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

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

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

14                   “(14) *lead and coordinate Federal efforts to pro-*  
15 *mote national cybersecurity awareness; and”.*

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

                  “Sec. 2220F. *Cybersecurity awareness campaigns.*”.



Calendar No. 382

118<sup>TH</sup> CONGRESS  
2<sup>D</sup> 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