

Calendar No. 291

118TH CONGRESS
1ST SESSION

S. 2201

To increase knowledge and awareness of best practices to reduce cybersecurity risks in the United States.

IN THE SENATE OF THE UNITED STATES

JUNE 22, 2023

Ms. KLOBUCHAR (for herself and Mr. THUNE) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

DECEMBER 13, 2023

Reported by Ms. CANTWELL, with an amendment

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

A BILL

To increase knowledge and awareness of best practices to reduce cybersecurity risks 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 “~~American Cybersecu-~~
5 ~~rity Literacy Act~~”.

1 **SEC. 2. CYBERSECURITY LITERACY CAMPAIGN.**

2 (a) IN GENERAL.—The Secretary of Commerce, in
3 consultation with the Director of the Cybersecurity and
4 Infrastructure Security Agency, shall develop and conduct
5 a cybersecurity literacy campaign described in subsection
6 (b), which the Secretary of Commerce shall make available
7 in multiple languages and formats, if practicable, to in-
8 crease the knowledge and awareness of citizens of the
9 United States of best practices to reduce cybersecurity
10 risks.

11 (b) ELEMENTS.—In carrying out subsection (a), the
12 Secretary of Commerce, in consultation with the Director
13 of the Cybersecurity and Infrastructure Security Agency,
14 shall—

15 (1) educate citizens of the United States with
16 respect to how to prevent and mitigate a cyberattack
17 or cybersecurity risk, including by—

18 (A) instructing citizens of the United
19 States with respect to how to identify—

20 (i) a phishing email or message; and
21 (ii) a secure website;

22 (B) instructing citizens of the United
23 States about the benefits of changing default
24 passwords on any hardware or software tech-
25 nology;

1 (C) encouraging the use of cybersecurity
2 tools, including—

- 3 (i) multi-factor authentication;
4 (ii) a complex password;
5 (iii) anti-virus software;
6 (iv) patching or updating software
7 and applications; and
8 (v) a virtual private network;

9 (D) identifying a device that could pose
10 possible cybersecurity risks, including—

- 11 (i) a personal computer;
12 (ii) a smartphone;
13 (iii) a tablet;
14 (iv) a Wi-Fi router;
15 (v) a smart home appliance;
16 (vi) a webcam;
17 (vii) an internet-connected monitor; or
18 (viii) any other device that can be con-
19 nected to the internet, including any mo-
20 bile device other than a smartphone or tab-
21 let;

22 (E) encouraging citizens of the United
23 States to—

- 24 (i) regularly review mobile application
25 permissions;

- 1 (ii) decline any privilege request from
 2 a mobile application that is unnecessary;
- 3 (iii) download an application only
 4 from a trusted vendor or source; and
- 5 (iv) consider the life cycle of a product
 6 and the commitment of a developer to pro-
 7 viding security updates during the expected
 8 period of use of a connected device; and
- 9 (F) identifying any potential cybersecurity
 10 risk related to using a publicly available Wi-Fi
 11 network and any method a user may use to
 12 limit such risks; and
- 13 (2) encourage citizens of the United States to
 14 use any resource to help mitigate the cybersecurity
 15 risks described in this subsection.

16 **SECTION 1. SHORT TITLE.**

17 *This Act may be cited as the “American Cybersecurity*
 18 *Literacy Act”.*

19 **SEC. 2. CYBERSECURITY LITERACY CAMPAIGN.**

20 (a) *IN GENERAL.*—*The Director of the National Insti-*
 21 *tute of Standards and Technology shall, in consultation*
 22 *with the Director of the Cybersecurity and Infrastructure*
 23 *Security Agency, develop and conduct a cybersecurity lit-*
 24 *eracy campaign described in subsection (b), which the Di-*
 25 *rector of the National Institute of Standards and Tech-*

1 *nology shall make available in multiple languages and for-*
2 *mats, if practicable, to increase the knowledge and aware-*
3 *ness of citizens of the United States of best practices to re-*
4 *duce cybersecurity risks.*

5 *(b) ELEMENTS.—In carrying out subsection (a), the*
6 *Director of the National Institute of Science and Tech-*
7 *nology, in consultation with the Director of the Cybersecu-*
8 *rity and Infrastructure Security Agency, shall—*

9 *(1) educate citizens of the United States with re-*
10 *spect to how to prevent and mitigate a cyberattack or*
11 *cybersecurity risk, including by—*

12 *(A) instructing citizens of the United States*
13 *with respect to how to identify—*

14 *(i) a phishing email or message; and*

15 *(ii) a secure website;*

16 *(B) instructing citizens of the United States*
17 *about the benefits of changing default passwords*
18 *on any hardware or software technology;*

19 *(C) encouraging the use of cybersecurity*
20 *tools, including—*

21 *(i) multi-factor authentication;*

22 *(ii) a complex password;*

23 *(iii) anti-virus software;*

24 *(iv) patching or updating software and*
25 *applications; and*

1 (v) a virtual private network;

2 (D) identifying a device that could pose
3 possible cybersecurity risks, including—

4 (i) a personal computer;

5 (ii) a smartphone;

6 (iii) a tablet;

7 (iv) a Wi-Fi router;

8 (v) a smart home appliance;

9 (vi) a webcam;

10 (vii) an internet-connected monitor; or

11 (viii) any other device that can be con-

12 nected to the internet, including any mobile

13 device other than a smartphone or tablet;

14 (E) encouraging citizens of the United

15 States to—

16 (i) regularly review mobile application
17 permissions;

18 (ii) decline any privilege request from
19 a mobile application that is unnecessary;

20 (iii) download an application only
21 from a trusted vendor or source; and

22 (iv) consider the life cycle of a product
23 and the commitment of a developer to pro-

24 viding security updates during the expected

25 period of use of a connected device; and

1 (F) identifying any potential cybersecurity
2 risk related to using a publicly available Wi-Fi
3 network and any method a user may use to limit
4 such risks; and

5 (2) encourage citizens of the United States to use
6 any resource that is developed as a result of this lit-
7 eracy campaign to help mitigate the cybersecurity
8 risks described in this subsection.

9 (c) *EXISTING AUTHORIZED AMOUNTS.*—No additional
10 funds are authorized to be appropriated for the purpose of
11 carrying out this Act.

Calendar No. 291

118TH CONGRESS
1ST Session

S. 2201

A BILL

To increase knowledge and awareness of best practices to reduce cybersecurity risks in the United States.

DECEMBER 13, 2023

Reported with an amendment