

117TH CONGRESS
2D SESSION

H. R. 6541

To require the Director of the Cybersecurity and Infrastructure Security Agency to establish cybersecurity guidance for small organizations, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 1, 2022

Ms. ESHOO (for herself, Mr. TIMMONS, Mr. RASKIN, and Mr. CASE) introduced the following bill; which was referred to the Committee on Small Business, and in addition to the Committee on Homeland Security, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To require the Director of the Cybersecurity and Infrastructure Security Agency to establish cybersecurity guidance for small organizations, and for other purposes.

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 “Improving Cybersecu-
5 rity of Small Businesses, Nonprofits, and Local Govern-
6 ments Act”.

1 **SEC. 2. IMPROVING CYBERSECURITY OF SMALL ENTITIES.**

2 (a) DEFINITIONS.—In this section:

3 (1) ADMINISTRATOR.—The term “Adminis-
4 trator” means the Administrator of the Small Busi-
5 ness Administration.

6 (2) ANNUAL CYBERSECURITY REPORT; SMALL
7 BUSINESS; SMALL ENTITY; SMALL GOVERNMENTAL
8 JURISDICTION; SMALL ORGANIZATION.—The terms
9 “annual cybersecurity report”, “small business”,
10 “small entity”, “small governmental jurisdiction”,
11 and “small organization” have the meanings given
12 those terms in section 2220D of the Homeland Se-
13 curity Act of 2002, as added by subsection (b).

14 (3) CISA.—The term “CISA” means the Cy-
15 bersecurity and Infrastructure Security Agency.

16 (4) COMMISSION.—The term “Commission”
17 means the Federal Trade Commission.

18 (5) SECRETARY.—The term “Secretary” means
19 the Secretary of Commerce.

20 (b) ANNUAL REPORT.—

21 (1) AMENDMENT.—Subtitle A of title XXII of
22 the Homeland Security Act of 2002 (6 U.S.C. 651
23 et seq.) is amended by adding at the end the fol-
24 lowing:

1 **“SEC. 2220D. ANNUAL CYBERSECURITY REPORT FOR**
2 **SMALL ENTITIES.**

3 “(a) DEFINITIONS.—

4 “(1) ADMINISTRATION.—The term ‘Administra-
5 tion’ means the Small Business Administration.

6 “(2) ADMINISTRATOR.—The term ‘Adminis-
7 trator’ means the Administrator of the Administra-
8 tion.

9 “(3) ANNUAL CYBERSECURITY REPORT.—The
10 term ‘annual cybersecurity report’ means the annual
11 cybersecurity report published and promoted under
12 subsections (b) and (c), respectively.

13 “(4) COMMISSION.—The term ‘Commission’
14 means the Federal Trade Commission.

15 “(5) ELECTRONIC DEVICE.—The term ‘elec-
16 tronic device’ means any electronic equipment that
17 is—

18 “(A) used by an employee or contractor of
19 a small entity for the purpose of performing
20 work for the small entity;

21 “(B) capable of connecting to the internet
22 or another communication network; and

23 “(C) capable of sending, receiving, or proc-
24 essing personal information.

25 “(6) NIST.—The term ‘NIST’ means the Na-
26 tional Institute of Standards and Technology.

1 “(7) SMALL BUSINESS.—The term ‘small busi-
2 ness’ has the meaning given the term ‘small business
3 concern’ under section 3 of the Small Business Act
4 (15 U.S.C. 632).

5 “(8) SMALL ENTITY.—The term ‘small entity’
6 means—

7 “(A) a small business;

8 “(B) a small governmental jurisdiction;

9 and

10 “(C) a small organization.

11 “(9) SMALL GOVERNMENTAL JURISDICTION.—

12 The term ‘small governmental jurisdiction’ means
13 governments of cities, counties, towns, townships,
14 villages, school districts, or special districts with a
15 population of less than 50,000.

16 “(10) SMALL ORGANIZATION.—The term ‘small
17 organization’ means any not-for-profit enterprise
18 that is independently owned and operated and is not
19 dominant in its field.

20 “(b) ANNUAL CYBERSECURITY REPORT.—

21 “(1) IN GENERAL.—Not later than 180 days
22 after the date of enactment of this section, and not
23 less frequently than annually thereafter, the Director
24 shall publish a report for small entities that docu-
25 ments and promotes evidence-based cybersecurity

1 policies and controls for use by small entities, which
2 shall—

3 “(A) include basic controls that have the
4 most impact in protecting small entities against
5 common cybersecurity threats and risks;

6 “(B) include protocols and policies to ad-
7 dress common cybersecurity threats and risks
8 posed by electronic devices, regardless of wheth-
9 er the electronic devices are—

10 “(i) issued by the small entity to em-
11 ployees and contractors of the small entity;

12 or

13 “(ii) personal to the employees and
14 contractors of the small entity; and

15 “(C) recommend, as practicable—

16 “(i) measures to improve the cyberse-
17 curity of small entities; and

18 “(ii) configurations and settings for
19 some of the most commonly used software
20 that can improve the cybersecurity of small
21 entities.

22 “(2) EXISTING RECOMMENDATIONS.—The Di-
23 rector shall ensure that each annual cybersecurity
24 report published under paragraph (1) incorporates—

1 “(A) cybersecurity resources developed by
2 NIST, as required by the NIST Small Business
3 Cybersecurity Act (Public Law 115–236); and

4 “(B) the most recent version of the Cyber-
5 security Framework, or successor resource,
6 maintained by NIST.

7 “(3) CONSIDERATION FOR SPECIFIC TYPES OF
8 SMALL ENTITIES.—The Director may include and
9 prioritize the development of cybersecurity rec-
10 ommendations, as required under paragraph (1), ap-
11 propriate for specific types of small entities in addi-
12 tion to recommendations applicable for all small en-
13 tities.

14 “(4) CONSULTATION.—In publishing the annual
15 cybersecurity report under paragraph (1), the Direc-
16 tor shall, to the degree practicable and as appro-
17 priate, consult with—

18 “(A) the Administrator, the Secretary of
19 Commerce, the Commission, and the Director of
20 NIST;

21 “(B) small entities, insurers, State govern-
22 ments, companies that work with small entities,
23 and academic and Federal and non-Federal ex-
24 perts in cybersecurity; and

1 “(C) any other entity as determined appro-
2 priate by the Director.

3 “(c) PROMOTION OF ANNUAL CYBERSECURITY RE-
4 PORT FOR SMALL BUSINESSES.—

5 “(1) PUBLICATION.—The annual cybersecurity
6 report, and previous versions of the report as appro-
7 priate, published under subsection (b)(1) shall be—

8 “(A) made available, prominently and free
9 of charge, on the public website of the Agency;
10 and

11 “(B) linked to from relevant portions of
12 the websites of the Administration and the Mi-
13 nority Business Development Agency, as deter-
14 mined by the Administrator and the Director of
15 the Minority Business Development Agency, re-
16 spectively.

17 “(2) PROMOTION GENERALLY.—The Director,
18 the Administrator, and the Secretary of Commerce
19 shall, to the degree practicable, promote the annual
20 cybersecurity report through relevant resources that
21 are intended for or known to be regularly used by
22 small entities, including agency documents, websites,
23 and events.

24 “(d) TRAINING AND TECHNICAL ASSISTANCE.—The
25 Director, the Administrator, and the Director of the Mi-

1 nority Business Development Agency shall make available
2 to employees of small entities voluntary training and tech-
3 nical assistance on how to implement the recommenda-
4 tions of the annual cybersecurity report.”.

5 (2) TECHNICAL AND CONFORMING AMEND-
6 MENT.—The table of contents in section 1(b) of the
7 Homeland Security Act of 2002 (Public 107–296;
8 116 Stat. 2135) is amended by inserting after the
9 item relating to section 2220C the following:

“Sec. 2220D. Annual cybersecurity report for small entities.”.

10 (c) REPORT TO CONGRESS.—

11 (1) IN GENERAL.—Not later than 1 year after
12 the date of enactment of this Act, and annually
13 thereafter for 10 years, the Secretary shall submit to
14 Congress a report describing methods to improve the
15 cybersecurity of small entities, including through the
16 adoption of policies, controls, and classes of products
17 and services that have been demonstrated to reduce
18 cybersecurity risk.

19 (2) MATTERS TO BE INCLUDED.—The report
20 required under paragraph (1) shall—

21 (A) identify barriers or challenges for
22 small entities in purchasing or acquiring classes
23 of products and services that promote the cy-
24 bersecurity of small entities;

1 (B) assess market availability, market pric-
2 ing, and affordability of classes of products and
3 services that promote the cybersecurity of small
4 entities, with particular attention to identifying
5 high-risk and underserved sectors or regions;

6 (C) estimate the costs and benefits of poli-
7 cies that promote the cybersecurity of small en-
8 tities, including—

9 (i) tax breaks;

10 (ii) grants and subsidies; and

11 (iii) other incentives as determined
12 appropriate by the Secretary;

13 (D) describe evidence-based cybersecurity
14 controls and policies that improve the cyberse-
15 curity of small entities;

16 (E) with respect to the incentives described
17 in subparagraph (C), recommend measures that
18 can effectively improve cybersecurity at scale
19 for small entities; and

20 (F) include any other matters as the Sec-
21 retary determines relevant.

22 (3) SPECIFIC SECTORS OF SMALL ENTITIES.—

23 In preparing the report required under paragraph
24 (1), the Secretary may include matters applicable for

1 specific sectors of small entities in addition to mat-
2 ters applicable to all small entities.

3 (4) CONSULTATION.—In preparing the report
4 required under paragraph (1), the Secretary shall
5 consult with—

6 (A) the Administrator, the Director of
7 CISA, and the Commission; and

8 (B) small entities, insurers of risks related
9 to cybersecurity, State governments, cybersecu-
10 rity and information technology companies that
11 work with small entities, and academic and
12 Federal and non-Federal experts in cybersecu-
13 rity.

14 (d) PERIODIC CENSUS ON STATE OF CYBERSECU-
15 RITY OF SMALL BUSINESSES.—

16 (1) IN GENERAL.—Not later than 1 year after
17 the date of enactment of this Act, and not less fre-
18 quently than every 24 months thereafter for 10
19 years, the Administrator shall submit to Congress
20 and make publicly available data on the state of cy-
21 bersecurity of small businesses, including, to the ex-
22 tent practicable—

23 (A) adoption of the cybersecurity rec-
24 ommendations from the annual cybersecurity
25 report among small businesses;

1 (B) the most significant and widespread
2 cybersecurity threats facing small businesses;

3 (C) the amount small businesses spend on
4 cybersecurity products and services; and

5 (D) the personnel small businesses dedi-
6 cate to cybersecurity, including the amount of
7 total personnel time, whether by employees or
8 contractors, dedicated to cybersecurity efforts.

9 (2) VOLUNTARY PARTICIPATION.—In carrying
10 out paragraph (1), the Administrator shall collect
11 data from small businesses that participate on a vol-
12 untary basis.

13 (3) FORM.—The data required under para-
14 graph (1) shall be produced in unclassified form but
15 may contain a classified annex.

16 (4) CONSULTATION.—In preparing to collect
17 the data required under paragraph (1), the Adminis-
18 trator shall consult with—

19 (A) the Secretary, the Director of CISA,
20 and the Commission; and

21 (B) small businesses, insurers of risks re-
22 lated to cybersecurity, cybersecurity and infor-
23 mation technology companies that work with
24 small businesses, and academic and Federal
25 and non-Federal experts in cybersecurity.

1 (5) PRIVACY.—In carrying out this subsection,
2 the Administrator shall ensure that any publicly
3 available data is anonymized and does not reveal
4 personally identifiable information.

5 (e) RULE OF CONSTRUCTION.—Nothing in this sec-
6 tion or the amendments made by this section shall be con-
7 strued to provide any additional regulatory authority to
8 CISA.

○