

Calendar No. 573

117TH CONGRESS
2^D SESSION

S. 2483

[Report No. 117–217]

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

IN THE SENATE OF THE UNITED STATES

JULY 27, 2021

Ms. ROSEN (for herself, Mr. CORNYN, Mr. OSSOFF, and Ms. HASSAN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

DECEMBER 5, 2022

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 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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Improving Cybersecu-
3 rity of Small Organizations Act of 2021”.

4 **SEC. 2. IMPROVING CYBERSECURITY OF SMALL ORGANIZA-**
5 **TIONS.**

6 (a) **DEFINITIONS.**—In this section:

7 (1) **ADMINISTRATION.**—The term “Administra-
8 tion” means the Small Business Administration.

9 (2) **ADMINISTRATOR.**—The term “Adminis-
10 trator” means the Administrator of the Administra-
11 tion.

12 (3) **COMMISSION.**—The term “Commission”
13 means the Federal Trade Commission.

14 (4) **CONNECTED DEVICE.**—The term “con-
15 nected device” means any electronic equipment that
16 is—

17 (A) primarily designed for or marketed to
18 consumers;

19 (B) capable of connecting to the internet
20 or another communication network; and

21 (C) capable of sending, receiving, or proc-
22 essing personal information.

23 (5) **CYBERSECURITY GUIDANCE.**—The term
24 “cybersecurity guidance” means the cybersecurity
25 guidance maintained and promoted under sub-
26 sections (b) and (c), respectively.

1 (6) DIRECTOR.—The term “Director” means
2 the Director of the Cybersecurity and Infrastructure
3 Security Agency.

4 (7) NIST.—The term “NIST” means the Na-
5 tional Institute of Standards and Technology.

6 (8) SECRETARY.—The term “Secretary” means
7 the Secretary of Commerce.

8 (9) SMALL BUSINESS.—The term “small busi-
9 ness” has the meaning given the term “small busi-
10 ness concern” in section 3 of the Small Business Act
11 (15 U.S.C. 632).

12 (10) SMALL GOVERNMENTAL JURISDICTION.—
13 The term “small governmental jurisdiction” has the
14 meaning given the term in section 601 of title 5,
15 United States Code.

16 (11) SMALL NONPROFIT.—The term “small
17 nonprofit” has the meaning given the term “small
18 organization” in section 601 of title 5, United States
19 Code.

20 (12) SMALL ORGANIZATION.—The term “small
21 organization” means an organization that is unlikely
22 to employ a specialist in cybersecurity, including—

23 (A) a small business;

24 (B) a small nonprofit; and

25 (C) a small governmental jurisdiction.

1 (b) ~~CYBERSECURITY GUIDANCE.—~~

2 (1) ~~IN GENERAL.—~~The Director shall maintain
3 cybersecurity guidance that documents and promotes
4 evidence-based cybersecurity policies and controls for
5 use by small organizations, which shall—

6 (A) include simple, basic controls that have
7 the most impact in protecting small organiza-
8 tions against common cybersecurity threats and
9 risks;

10 (B) include guidance to address common
11 cybersecurity threats and risks posed by con-
12 nected devices that are personal to the employ-
13 ees and contractors of small organizations, as
14 well as connected devices that are issued to
15 those employees and contractors by small orga-
16 nizations; and

17 (C) recommend—

18 (i) measures to improve the cybersecu-
19 rity of small organizations; and

20 (ii) configurations and settings for
21 some of the most commonly used software
22 that can improve the cybersecurity of small
23 organizations.

1 (2) ~~CONSISTENCY.~~—The Director shall ensure
2 the cybersecurity guidance maintained under para-
3 graph (1) is consistent with—

4 (A) cybersecurity resources developed by
5 NIST, as required by the NIST Small Business
6 Cybersecurity Act (Public Law 115–236); and

7 (B) the most recent version of the Cyberse-
8 curity Framework, or successor resource, main-
9 tained by NIST.

10 (3) ~~GUIDANCE FOR SPECIFIC TYPES OF SMALL~~
11 ~~ORGANIZATIONS.~~—The Director may include cyber-
12 security guidance, as required under paragraph (1),
13 appropriate for specific types of small organizations
14 in addition to guidance applicable for all small orga-
15 nizations.

16 (4) ~~UPDATES.~~—

17 (A) ~~IN GENERAL.~~—The Director shall re-
18 view the cybersecurity guidance maintained
19 under paragraph (1) not less frequently than
20 annually and update the cybersecurity guidance
21 as appropriate.

22 (B) ~~CONSULTATION.~~—In updating the cy-
23 bersecurity guidance under subparagraph (A),
24 the Director shall, to the degree practicable and
25 as appropriate, consult with—

1 (i) the Administrator, the Secretary,
2 and the Commission;

3 (ii) small organizations, insurers,
4 State governments, companies that work
5 with small organizations, and academic
6 and Federal and non-Federal experts in
7 cybersecurity; and

8 (iii) any other entity as determined by
9 the Director.

10 (5) USER INTERFACE.—As appropriate, the Di-
11 rector shall consult with experts regarding the de-
12 sign of a user interface for the cybersecurity guid-
13 ance.

14 (c) PROMOTION OF CYBERSECURITY GUIDANCE FOR
15 SMALL BUSINESSES.—

16 (1) PUBLIC AVAILABILITY.—The cybersecurity
17 guidance maintained under subsection (b)(1) shall
18 be—

19 (A) made available, prominently and free
20 of charge, on the public website of the Cyberse-
21 curity Infrastructure Security Agency; and

22 (B) linked to from relevant portions of the
23 websites of the Administration and the Minority
24 Business Development Agency.

1 (2) PROMOTION GENERALLY.—The Director,
 2 the Administrator, and the Secretary shall, to the
 3 degree practicable, promote the cybersecurity guid-
 4 ance through relevant resources that are intended
 5 for or known to be regularly used by small organiza-
 6 tions, including agency documents, websites, and
 7 events.

8 (d) REPORT ON INCENTIVIZING CYBERSECURITY FOR
 9 SMALL ORGANIZATIONS.—

10 (1) IN GENERAL.—Not later than 1 year after
 11 the date of enactment of this Act, the Secretary
 12 shall submit to Congress a report describing meth-
 13 ods to incentivize small organizations to improve
 14 their cybersecurity, including through the adoption
 15 of policies, controls, products and services that have
 16 been demonstrated to reduce cybersecurity risk.

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

19 (A) identify barriers or challenges for
 20 small organizations in purchasing or acquiring
 21 products and services that promote the cyberse-
 22 curity;

23 (B) assess market availability, market prie-
 24 ing, and affordability of products and services
 25 that promote the cybersecurity for small organi-

zations, with particular attention to identifying high-risk and underserved sectors or regions;

(C) estimate the cost of tax breaks, grants, subsidies, or other incentives to increase the adoption of policies and controls or acquisition of products and services that promote the cybersecurity of small organizations;

(D) as practicable, consult the certifications and requirement for cloud services described in the final report of the Cyberspace Solarium Commission established under section 1652 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232, 132 Stat. 2140);

(E) describe evidence-based cybersecurity controls and policies that improve cybersecurity for small organizations;

(F) with respect to the incentives described in subparagraph (C), recommend measures that can effectively improve cybersecurity at scale for small organizations; and

(G) include any other matters as the Secretary determines relevant.

(3) GUIDANCE FOR SPECIFIC TYPES OF SMALL ORGANIZATIONS.—In preparing the report required

under paragraph (1), the Secretary may include matters applicable for specific types of small organizations in addition to matters applicable to all small organizations.

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

(A) the Administrator, the Director, and the Commission; and

(B) small organizations, insurers of risks related to cybersecurity, State governments, cybersecurity and information technology companies that work with small organizations, and academic and Federal and non-Federal experts in cybersecurity.

(c) PERIODIC CENSUS ON STATE OF CYBERSECURITY OF SMALL BUSINESSES.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act and not less frequently than every 24 months thereafter for not more than 10 years, the Administrator shall submit to Congress and make publicly available data on the state of cybersecurity of small businesses, including—

1 (A) adoption of the cybersecurity guidance
2 among small businesses;

3 (B) the most significant and widespread
4 cybersecurity threats facing small businesses;

5 (C) the amount small businesses spend on
6 cybersecurity products and services; and

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

11 (2) FORM.—The report required under para-
12 graph (1) shall be produced in unclassified form but
13 may contain a classified annex.

14 (3) CONSULTATION.—In preparing the report
15 required under paragraph (1), the Administrator
16 shall consult with—

17 (A) the Secretary, the Director, and the
18 Commission; and

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

1 **SECTION 1. SHORT TITLE.**

2 *This Act may be cited as the “Improving Cybersecurity*
 3 *of Small Businesses, Nonprofits, and Local Governments*
 4 *Act of 2021”.*

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

6 (a) *DEFINITIONS.—In this section:*

7 (1) *ADMINISTRATOR.—The term “Adminis-*
 8 *trator” means the Administrator of the Small Busi-*
 9 *ness Administration.*

10 (2) *ANNUAL CYBERSECURITY REPORT; SMALL*
 11 *BUSINESS; SMALL ENTITY; SMALL GOVERNMENTAL JU-*
 12 *RISDICTION; SMALL ORGANIZATION.—The terms “an-*
 13 *ual cybersecurity report”, “small business”, “small*
 14 *entity”, “small governmental jurisdiction”, and*
 15 *“small organization” have the meanings given those*
 16 *terms in section 2220D of the Homeland Security Act*
 17 *of 2002, as added by subsection (b).*

18 (3) *CISA.—The term “CISA” means the Cyber-*
 19 *security and Infrastructure Security Agency.*

20 (4) *COMMISSION.—The term “Commission”*
 21 *means the Federal Trade Commission.*

22 (5) *SECRETARY.—The term “Secretary” means*
 23 *the Secretary of Commerce.*

24 (b) *ANNUAL REPORT.—*

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

4 **“SEC. 2220D. ANNUAL CYBERSECURITY REPORT FOR SMALL**
 5 **ENTITIES.**

6 “(a) *DEFINITIONS.*—

7 “(1) *ADMINISTRATION.*—*The term ‘Administra-*
 8 *tion’ means the Small Business Administration.*

9 “(2) *ADMINISTRATOR.*—*The term ‘Adminis-*
 10 *trator’ means the Administrator of the Administra-*
 11 *tion.*

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

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

18 “(5) *ELECTRONIC DEVICE.*—*The term ‘electronic*
 19 *device’ means any electronic equipment that is—*

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

23 “(B) *capable of connecting to the internet or*
 24 *another communication network; and*

1 “(C) *capable of sending, receiving, or proc-*
 2 *essing personal information.*

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

5 “(7) *SMALL BUSINESS.*—*The term ‘small busi-*
 6 *ness’ has the meaning given the term ‘small business*
 7 *concern’ in section 3 of the Small Business Act (15*
 8 *U.S.C. 632).*

9 “(8) *SMALL ENTITY.*—*The term ‘small entity’*
 10 *means—*

11 “(A) *a small business;*

12 “(B) *a small governmental jurisdiction; and*

13 “(C) *a small organization.*

14 “(9) *SMALL GOVERNMENTAL JURISDICTION.*—
 15 *The term ‘small governmental jurisdiction’ means*
 16 *governments of cities, counties, towns, townships, vil-*
 17 *lages, school districts, or special districts with a pop-*
 18 *ulation of less than 50,000.*

19 “(10) *SMALL ORGANIZATION.*—*The term ‘small*
 20 *organization’ means any not-for-profit enterprise that*
 21 *is independently owned and operated and is not dom-*
 22 *inant in its field.*

23 “(b) *ANNUAL CYBERSECURITY REPORT.*—

24 “(1) *IN GENERAL.*—*Not later than 180 days*
 25 *after the date of enactment of this section, and not*

1 *less frequently than annually thereafter, the Director*
2 *shall publish a report for small entities that docu-*
3 *ments and promotes evidence-based cybersecurity poli-*
4 *cies and controls for use by small entities, which*
5 *shall—*

6 “(A) *include basic controls that have the*
7 *most impact in protecting small entities against*
8 *common cybersecurity threats and risks;*

9 “(B) *include protocols and policies to ad-*
10 *dress common cybersecurity threats and risks*
11 *posed by electronic devices, regardless of whether*
12 *the electronic devices are—*

13 “(i) *issued by the small entity to em-*
14 *ployees and contractors of the small entity;*
15 *or*

16 “(ii) *personal to the employees and*
17 *contractors of the small entity; and*

18 “(C) *recommend, as practicable—*

19 “(i) *measures to improve the cybersecu-*
20 *rity of small entities; and*

21 “(ii) *configurations and settings for*
22 *some of the most commonly used software*
23 *that can improve the cybersecurity of small*
24 *entities.*

1 “(2) *EXISTING RECOMMENDATIONS.*—*The Direc-*
2 *tor shall ensure that each annual cybersecurity report*
3 *published under paragraph (1) incorporates—*

4 “(A) *cybersecurity resources developed by*
5 *NIST, as required by the NIST Small Business*
6 *Cybersecurity Act (Public Law 115–236; 132*
7 *Stat. 2444); and*

8 “(B) *the most recent version of the Cyberse-*
9 *curity Framework, or a successor resource, main-*
10 *tained by NIST.*

11 “(3) *CONSIDERATION FOR SPECIFIC TYPES OF*
12 *SMALL ENTITIES.*—*The Director may include and*
13 *prioritize the development of cybersecurity rec-*
14 *ommendations, as required under paragraph (1), ap-*
15 *propriate for specific types of small entities in addi-*
16 *tion to recommendations applicable for all small enti-*
17 *ties.*

18 “(4) *CONSULTATION.*—*In publishing the annual*
19 *cybersecurity report under paragraph (1), the Direc-*
20 *tor shall, to the degree practicable and as appro-*
21 *priate, consult with—*

22 “(A) *the Administrator, the Secretary of*
23 *Commerce, the Commission, and the Director of*
24 *NIST;*

1 “(B) *small entities, insurers, State govern-*
 2 *ments, companies that work with small entities,*
 3 *and academic and Federal and non-Federal ex-*
 4 *perts in cybersecurity; and*

5 “(C) *any other entity as determined appro-*
 6 *priate by the Director.*

7 “(c) *PROMOTION OF ANNUAL CYBERSECURITY REPORT*
 8 *FOR SMALL BUSINESSES.—*

9 “(1) *PUBLICATION.—The annual cybersecurity*
 10 *report, and previous versions of the report as appro-*
 11 *priate, published under subsection (b)(1) shall be—*

12 “(A) *made available, prominently and free*
 13 *of charge, on the public website of the Agency;*
 14 *and*

15 “(B) *linked to from relevant portions of the*
 16 *websites of the Administration and the Minority*
 17 *Business Development Agency, as determined by*
 18 *the Administrator and the Director of the Minor-*
 19 *ity Business Development Agency, respectively.*

20 “(2) *PROMOTION GENERALLY.—The Director, the*
 21 *Administrator, and the Secretary of Commerce shall,*
 22 *to the degree practicable, promote the annual cyberse-*
 23 *curity report through relevant resources that are in-*
 24 *tended for or known to be regularly used by small en-*

1 *tities, including agency documents, websites, and*
 2 *events.*

3 “(d) *TRAINING AND TECHNICAL ASSISTANCE.—The*
 4 *Director, the Administrator, and the Director of the Minor-*
 5 *ity Business Development Agency shall make available to*
 6 *employees of small entities voluntary training and technical*
 7 *assistance on how to implement the recommendations of the*
 8 *annual cybersecurity report.”.*

9 (2) *TECHNICAL AND CONFORMING AMEND-*
 10 *MENT.—The table of contents in section 1(b) of the*
 11 *Homeland Security Act of 2002 (Public 107–296; 116*
 12 *Stat. 2135) is amended by inserting after the item re-*
 13 *lating to section 2220C the following:*

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

14 (c) *REPORT TO CONGRESS.—*

15 (1) *IN GENERAL.—Not later than 1 year after*
 16 *the date of enactment of this Act, and annually there-*
 17 *after for 10 years, the Secretary shall submit to Con-*
 18 *gress a report describing methods to improve the cy-*
 19 *bersecurity of small entities, including through the*
 20 *adoption of policies, controls, and classes of products*
 21 *and services that have been demonstrated to reduce*
 22 *cybersecurity risk.*

23 (2) *MATTERS TO BE INCLUDED.—The report re-*
 24 *quired under paragraph (1) shall—*

1 (A) identify barriers or challenges for small
2 entities in purchasing or acquiring classes of
3 products and services that promote the cybersecu-
4 rity of small entities;

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

10 (C) estimate the costs and benefits of poli-
11 cies that promote the cybersecurity of small enti-
12 ties, including—

13 (i) tax breaks;

14 (ii) grants and subsidies; and

15 (iii) other incentives as determined ap-
16 propriate by the Secretary;

17 (D) describe evidence-based cybersecurity
18 controls and policies that improve the cybersecu-
19 rity of small entities;

20 (E) with respect to the incentives described
21 in subparagraph (C), recommend measures that
22 can effectively improve cybersecurity at scale for
23 small entities; and

24 (F) include any other matters as the Sec-
25 retary determines relevant.

1 (3) *SPECIFIC SECTORS OF SMALL ENTITIES.*—In
 2 *preparing the report required under paragraph (1),*
 3 *the Secretary may include matters applicable for spe-*
 4 *cific sectors of small entities in addition to matters*
 5 *applicable to all small entities.*

6 (4) *CONSULTATION.*—In preparing the report re-
 7 *quired under paragraph (1), the Secretary shall con-*
 8 *sult with—*

9 (A) *the Administrator, the Director of*
 10 *CISA, and the Commission; and*

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

16 (d) *PERIODIC CENSUS ON STATE OF CYBERSECURITY*
 17 *OF SMALL BUSINESSES.*—

18 (1) *IN GENERAL.*—Not later than 1 year after
 19 *the date of enactment of this Act, and not less fre-*
 20 *quently than every 24 months thereafter for 10 years,*
 21 *the Administrator shall submit to Congress and make*
 22 *publicly available data on the state of cybersecurity*
 23 *of small businesses, including, to the extent prac-*
 24 *ticable—*

1 (A) adoption of the cybersecurity rec-
 2 ommendations from the annual cybersecurity re-
 3 port among small businesses;

4 (B) the most significant and widespread cy-
 5 bersecurity threats facing small businesses;

6 (C) the amount small businesses spend on
 7 cybersecurity products and services; and

8 (D) the personnel small businesses dedicate
 9 to cybersecurity, including the amount of total
 10 personnel time, whether by employees or contrac-
 11 tors, dedicated to cybersecurity efforts.

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

16 (3) *FORM.*—The data required under paragraph
 17 (1) shall be produced in unclassified form but may
 18 contain a classified annex.

19 (4) *CONSULTATION.*—In preparing to collect the
 20 data required under paragraph (1), the Adminis-
 21 trator shall consult with—

22 (A) the Secretary, the Director of CISA,
 23 and the Commission; and

24 (B) small businesses, insurers of risks re-
 25 lated to cybersecurity, cybersecurity and infor-

1 *mation technology companies that work with*
2 *small businesses, and academic and Federal and*
3 *non-Federal experts in cybersecurity.*

4 (5) *PRIVACY.—In carrying out this subsection,*
5 *the Administrator shall ensure that any publicly*
6 *available data is anonymized and does not reveal per-*
7 *sonally identifiable information.*

8 (e) *RULE OF CONSTRUCTION.—Nothing in this section*
9 *or the amendments made by this section shall be construed*
10 *to provide any additional regulatory authority to CISA.*

Calendar No. 573

117TH CONGRESS
2^D Session

S. 2483

[Report No. 117-217]

A BILL

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

DECEMBER 5, 2022

Reported with an amendment