

AMENDMENT NO. \_\_\_\_\_ Calendar No. \_\_\_\_\_

Purpose: In the nature of a substitute.

**IN THE SENATE OF THE UNITED STATES—117th Cong., 2d Sess.**

**S. 2483**

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

Referred to the Committee on \_\_\_\_\_ and  
ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended  
to be proposed by Ms. ROSEN

Viz:

1 Strike all after the enacting clause and insert the fol-  
2 lowing:

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 of 2021”.

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

8 (a) DEFINITIONS.—In this section:

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

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

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

11           (4) COMMISSION.—The term “Commission”  
12 means the Federal Trade Commission.

13           (5) SECRETARY.—The term “Secretary” means  
14 the Secretary of Commerce.

15 (b) ANNUAL REPORT.—

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

20 **“SEC. 2220D. ANNUAL CYBERSECURITY REPORT FOR**  
21 **SMALL ENTITIES.**

22 “(a) DEFINITIONS.—

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

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

4           “(3) ANNUAL CYBERSECURITY REPORT.—The  
5           term ‘annual cybersecurity report’ means the annual  
6           cybersecurity report published and promoted under  
7           subsections (b) and (c), respectively.

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

10          “(5) ELECTRONIC DEVICE.—The term ‘elec-  
11          tronic device’ means any electronic equipment that  
12          is—

13                 “(A) used by an employee or contractor of  
14                 a small entity for the purpose of performing  
15                 work for the small entity;

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

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

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

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

1           “(8) SMALL ENTITY.—The term ‘small entity’  
2 means—

3           “(A) a small business;

4           “(B) a small governmental jurisdiction;

5           and

6           “(C) a small organization.

7           “(9) SMALL GOVERNMENTAL JURISDICTION.—

8           The term ‘small governmental jurisdiction’ means  
9 governments of cities, counties, towns, townships,  
10 villages, school districts, or special districts with a  
11 population of less than 50,000.

12           “(10) SMALL ORGANIZATION.—The term ‘small  
13 organization’ means any not-for-profit enterprise  
14 that is independently owned and operated and is not  
15 dominant in its field.

16           “(b) ANNUAL CYBERSECURITY REPORT.—

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

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

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

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

10           or

11           “(ii) personal to the employees and  
12 contractors of the small entity; and

13           “(C) recommend, as practicable—

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

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

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

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

1           “(B) the most recent version of the Cyber-  
2           security Framework, or successor resource,  
3           maintained by NIST.

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

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

15                 “(A) the Administrator, the Secretary of  
16                 Commerce, the Commission, and the Director of  
17                 NIST;

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

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

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

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

4                   “(A) made available, prominently and free  
5                   of charge, on the public website of the Agency;  
6                   and

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

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

20           “(d) TRAINING AND TECHNICAL ASSISTANCE.—The  
21           Director, the Administrator, and the Director of the Mi-  
22           nority Business Development Agency shall make available  
23           to employees of small entities voluntary training and tech-  
24           nical assistance on how to implement the recommenda-  
25           tions of the annual cybersecurity report.”.

1           (2) TECHNICAL AND CONFORMING AMEND-  
2           MENT.—The table of contents in section 1(b) of the  
3           Homeland Security Act of 2002 (Public 107–296;  
4           116 Stat. 2135) is amended by inserting after the  
5           item relating to section 2220C the following:

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

6           (c) REPORT TO CONGRESS.—

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

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

17                (A) identify barriers or challenges for  
18                small entities in purchasing or acquiring classes  
19                of products and services that promote the cy-  
20                bersecurity of small entities;

21                (B) assess market availability, market pric-  
22                ing, and affordability of classes of products and  
23                services that promote the cybersecurity of small  
24                entities, with particular attention to identifying  
25                high-risk and underserved sectors or regions;



1 (C) estimate the costs and benefits of poli-  
2 cies that promote the cybersecurity of small en-  
3 tities, including—

4 (i) tax breaks;

5 (ii) grants and subsidies; and

6 (iii) other incentives as determined  
7 appropriate by the Secretary;

8 (D) describe evidence-based cybersecurity  
9 controls and policies that improve the cyberse-  
10 curity of small entities;

11 (E) with respect to the incentives described  
12 in subparagraph (C), recommend measures that  
13 can effectively improve cybersecurity at scale  
14 for small entities; and

15 (F) include any other matters as the Sec-  
16 retary determines relevant.

17 (3) SPECIFIC SECTORS OF SMALL ENTITIES.—

18 In preparing the report required under paragraph  
19 (1), the Secretary may include matters applicable for  
20 specific sectors of small entities in addition to mat-  
21 ters applicable to all small entities.

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

1 (A) the Administrator, the Director of  
2 CISA, and the Commission; and

3 (B) small entities, insurers of risks related  
4 to cybersecurity, State governments, cybersecu-  
5 rity and information technology companies that  
6 work with small entities, and academic and  
7 Federal and non-Federal experts in cybersecu-  
8 rity.

9 (d) PERIODIC CENSUS ON STATE OF CYBERSECU-  
10 RITY OF SMALL BUSINESSES.—

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

18 (A) adoption of the cybersecurity rec-  
19 ommendations from the annual cybersecurity  
20 report among small businesses;

21 (B) the most significant and widespread  
22 cybersecurity threats facing small businesses;

23 (C) the amount small businesses spend on  
24 cybersecurity products and services; and

1 (D) the personnel small businesses dedi-  
2 cate to cybersecurity, including the amount of  
3 total personnel time, whether by employees or  
4 contractors, dedicated to cybersecurity efforts.

5 (2) VOLUNTARY PARTICIPATION.—In carrying  
6 out paragraph (1), the Administrator shall collect  
7 data from small businesses that participate on a vol-  
8 untary basis.

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

12 (4) CONSULTATION.—In preparing to collect  
13 the data required under paragraph (1), the Adminis-  
14 trator shall consult with—

15 (A) the Secretary, the Director of CISA,  
16 and the Commission; and

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

22 (5) PRIVACY.—In carrying out this subsection,  
23 the Administrator shall ensure that any publicly  
24 available data is anonymized and does not reveal  
25 personally identifiable information.

1       (e) RULE OF CONSTRUCTION.—Nothing in this sec-  
2 tion or the amendments made by this section shall be con-  
3 strued to provide any additional regulatory authority to  
4 CISA.