

117TH CONGRESS
1ST SESSION

S. 2483

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 and Mr. CORNYN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

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 Organizations Act of 2021”.

6 **SEC. 2. IMPROVING CYBERSECURITY OF SMALL ORGANIZA-**
7 **TIONS.**

8 (a) DEFINITIONS.—In this section:

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

3 (2) ADMINISTRATOR.—The term “Adminis-
4 trator” means the Administrator of the Administra-
5 tion.

6 (3) COMMISSION.—The term “Commission”
7 means the Federal Trade Commission.

8 (4) CONNECTED DEVICE.—The term “con-
9 nected device” means any electronic equipment that
10 is—

11 (A) primarily designed for or marketed to
12 consumers;

13 (B) capable of connecting to the internet
14 or another communication network; and

15 (C) capable of sending, receiving, or proc-
16 essing personal information.

17 (5) CYBERSECURITY GUIDANCE.—The term
18 “cybersecurity guidance” means the cybersecurity
19 guidance maintained and promoted under sub-
20 sections (b) and (c), respectively.

21 (6) DIRECTOR.—The term “Director” means
22 the Director of the Cybersecurity and Infrastructure
23 Security Agency.

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

1 (8) SECRETARY.—The term “Secretary” means
2 the Secretary of Commerce.

3 (9) SMALL BUSINESS.—The term “small busi-
4 ness” has the meaning given the term “small busi-
5 ness concern” in section 3 of the Small Business Act
6 (15 U.S.C. 632).

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

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

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

18 (A) a small business;

19 (B) a small nonprofit; and

20 (C) a small governmental jurisdiction.

21 (b) CYBERSECURITY GUIDANCE.—

22 (1) IN GENERAL.—The Director shall maintain
23 cybersecurity guidance that documents and promotes
24 evidence-based cybersecurity policies and controls for
25 use by small organizations, which shall—

1 (A) include simple, basic controls that have
2 the most impact in protecting small organiza-
3 tions against common cybersecurity threats and
4 risks;

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

12 (C) recommend—

13 (i) measures to improve the cybersecu-
14 rity of small organizations; and

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

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

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

1 (B) the most recent version of the Cyberse-
2 curity Framework, or successor resource, main-
3 tained by NIST.

4 (3) GUIDANCE FOR SPECIFIC TYPES OF SMALL
5 ORGANIZATIONS.—The Director may include cyber-
6 security guidance, as required under paragraph (1),
7 appropriate for specific types of small organizations
8 in addition to guidance applicable for all small orga-
9 nizations.

10 (4) UPDATES.—

11 (A) IN GENERAL.—The Director shall re-
12 view the cybersecurity guidance maintained
13 under paragraph (1) not less frequently than
14 annually and update the cybersecurity guidance
15 as appropriate.

16 (B) CONSULTATION.—In updating the cy-
17 bersecurity guidance under subparagraph (A),
18 the Director shall, to the degree practicable and
19 as appropriate, consult with—

20 (i) the Administrator, the Secretary,
21 and the Commission;

22 (ii) small organizations, insurers,
23 State governments, companies that work
24 with small organizations, and academic

1 and Federal and non-Federal experts in
2 cybersecurity; and

3 (iii) any other entity as determined by
4 the Director.

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

9 (c) PROMOTION OF CYBERSECURITY GUIDANCE FOR
10 SMALL BUSINESSES.—

11 (1) PUBLIC AVAILABILITY.—The cybersecurity
12 guidance maintained under subsection (b)(1) shall
13 be—

14 (A) made available, prominently and free
15 of charge, on the public website of the Cyberse-
16 curity Infrastructure Security Agency; and

17 (B) linked to from relevant portions of the
18 websites of the Administration and the Minority
19 Business Development Agency.

20 (2) PROMOTION GENERALLY.—The Director,
21 the Administrator, and the Secretary shall, to the
22 degree practicable, promote the cybersecurity guid-
23 ance through relevant resources that are intended
24 for or known to be regularly used by small organiza-

1 tions, including agency documents, websites, and
2 events.

3 (d) REPORT ON INCENTIVIZING CYBERSECURITY FOR
4 SMALL ORGANIZATIONS.—

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

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

14 (A) identify barriers or challenges for
15 small organizations in purchasing or acquiring
16 products and services that promote the cyberse-
17 curity;

18 (B) assess market availability, market pric-
19 ing, and affordability of products and services
20 that promote the cybersecurity for small organi-
21 zations, with particular attention to identifying
22 high-risk and underserved sectors or regions;

23 (C) estimate the cost of tax breaks, grants,
24 subsidies, or other incentives to increase the
25 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.

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

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

6 (B) small organizations, insurers of risks
 7 related to cybersecurity, State governments, cy-
 8 bersecurity and information technology compa-
 9 nies that work with small organizations, and
 10 academic and Federal and non-Federal experts
 11 in cybersecurity.

12 (e) PERIODIC CENSUS ON STATE OF CYBERSECURITY
 13 OF SMALL BUSINESSES.—

14 (1) IN GENERAL.—Not later than 1 year after
 15 the date of enactment of this Act and not less fre-
 16 quently than every 24 months thereafter for not
 17 more than 10 years, the Administrator shall submit
 18 to Congress and make publicly available data on the
 19 state of cybersecurity of small businesses, includ-
 20 ing—

21 (A) adoption of the cybersecurity guidance
 22 among small businesses;

23 (B) the most significant and widespread
 24 cybersecurity threats facing small businesses;

1 (C) the amount small businesses spend on
2 cybersecurity products and services; and

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

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

10 (3) CONSULTATION.—In preparing the report
11 required under paragraph (1), the Administrator
12 shall consult with—

13 (A) the Secretary, the Director, and the
14 Commission; and

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

○