

116TH CONGRESS  
2D SESSION

# S. 4731

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

SEPTEMBER 24, 2020

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 2020”.

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) CYBERSECURITY GUIDANCE.—The term  
9           “cybersecurity guidance” means the cybersecurity  
10          guidance documented and promoted in the resource  
11          maintained under section 3(a).

12          (5) DIRECTOR.—The term “Director” means  
13          the Director of the Cybersecurity and Infrastructure  
14          Security Agency.

15          (6) NIST.—The term “NIST” means the Na-  
16          tional Institute of Standards and Technology.

17          (7) SECRETARY.—The term “Secretary” means  
18          the Secretary of Commerce.

19          (8) SMALL BUSINESS.—The term “small busi-  
20          ness” has the meaning given the term “small busi-  
21          ness concern” in section 3 of the Small Business Act  
22          (15 U.S.C. 632).

23          (9) SMALL GOVERNMENTAL JURISDICTION.—  
24          The term “small governmental jurisdiction” has the

1 meaning given the term in section 601 of title 5,  
2 United States Code.

3 (10) SMALL NONPROFIT.—The term “small  
4 nonprofit” has the meaning given the term “small  
5 organization” in section 601 of title 5, United States  
6 Code.

7 (11) SMALL ORGANIZATION.—The term “small  
8 organization” means an organization that is unlikely  
9 to employ a specialist in cybersecurity, including—

10 (A) a small business;

11 (B) a small nonprofit; and

12 (C) a small governmental jurisdiction.

13 (b) CYBERSECURITY GUIDANCE.—

14 (1) IN GENERAL.—The Director shall maintain  
15 cybersecurity guidance that documents and promotes  
16 evidence-based cybersecurity policies and controls for  
17 use by small organizations, which shall—

18 (A) include simple, basic controls that have  
19 the most impact in protecting small organiza-  
20 tions against common cybersecurity threats and  
21 risks;

22 (B) include guidance to address common  
23 cybersecurity threats and risks posed by elec-  
24 tronic devices that are personal to the employ-  
25 ees and contractors of small organizations, as

1 well as electronic devices that are issued to  
2 those employees and contractors by small orga-  
3 nizations; and

4 (C) recommend—

5 (i) measures to improve the cybersecu-  
6 rity of small organizations; and

7 (ii) configurations and settings for  
8 some of the most commonly used software  
9 that can improve the cybersecurity of small  
10 organizations.

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

14 (A) cybersecurity resources developed by  
15 NIST, as required by the NIST Small Business  
16 Cybersecurity Act (Public Law 115–236); and

17 (B) the most recent version of the Cyberse-  
18 curity Framework, or successor resource, main-  
19 tained by NIST.

20 (3) GUIDANCE FOR SPECIFIC TYPES OF SMALL  
21 ORGANIZATIONS.—The Director may include cyber-  
22 security guidance, as required under paragraph (1),  
23 appropriate for specific types of small organizations  
24 in addition to guidance applicable for all small orga-  
25 nizations.

1 (4) UPDATES.—

2 (A) IN GENERAL.—The Director shall re-  
3 view the cybersecurity guidance maintained  
4 under paragraph (1) not less frequently than  
5 annually and update the cybersecurity guidance  
6 as appropriate.

7 (B) CONSULTATION.—In updating the cy-  
8 bersecurity guidance under subparagraph (A),  
9 the Director shall, to the degree practicable and  
10 as appropriate, consult with—

11 (i) the Administrator, the Secretary,  
12 and the Commission;

13 (ii) small organizations, insurers,  
14 State governments, companies that work  
15 with small organizations, and academic  
16 and Federal and non-Federal experts in  
17 cybersecurity; and

18 (iii) any other entity as determined by  
19 the Director.

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

24 (c) PROMOTION OF CYBERSECURITY GUIDANCE FOR  
25 SMALL BUSINESSES.—

1           (1) PUBLIC AVAILABILITY.—The cybersecurity  
2 guidance maintained under subsection (b)(1) shall  
3 be—

4                   (A) made available, prominently and free  
5 of charge, on the public website of the Cyberse-  
6 curity Infrastructure Security Agency; and

7                   (B) linked to from relevant portions of the  
8 websites of the Administration and the Minority  
9 Business Development Agency.

10           (2) PROMOTION GENERALLY.—The Director,  
11 the Administrator, and the Secretary shall, to the  
12 degree practicable, promote the cybersecurity guid-  
13 ance through relevant resources that are intended  
14 for or known to be regularly used by small organiza-  
15 tions, including agency documents, websites, and  
16 events.

17           (d) REPORT ON INCENTIVIZING CYBERSECURITY FOR  
18 SMALL ORGANIZATIONS.—

19                   (1) IN GENERAL.—Not later than 1 year after  
20 the date of enactment of this Act, the Secretary  
21 shall submit to Congress a report describing meth-  
22 ods to incentivize small organizations to improve  
23 their cybersecurity, including through the adoption  
24 of policies, controls, products and services that have  
25 been demonstrated to reduce cybersecurity risk.

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

3           (A) identify barriers or challenges for  
4 small organizations in purchasing or acquiring  
5 products and services that promote the cyberse-  
6 curity;

7           (B) assess market availability, market pric-  
8 ing, and affordability of products and services  
9 that promote the cybersecurity for small organi-  
10 zations, with particular attention to identifying  
11 high-risk and underserved sectors or regions;

12           (C) estimate the cost of tax breaks, grants,  
13 subsidies, or other incentives to increase the  
14 adoption of policies and controls or acquisition  
15 of products and services that promote the cy-  
16 bersecurity of small organizations;

17           (D) as practicable, consult the certifi-  
18 cations and requirement for cloud services de-  
19 scribed in the final report of the Cyberspace So-  
20 larium Commission established under section  
21 1652 of the John S. McCain National Defense  
22 Authorization Act for Fiscal Year 2019 (Public  
23 Law 115–232; 132 Stat. 2140);

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

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

8           (G) include any other matters as the Sec-  
9 retary determines relevant.

10           (3) GUIDANCE FOR SPECIFIC TYPES OF SMALL  
11 ORGANIZATIONS.—In preparing the report required  
12 under paragraph (1), the Secretary may include  
13 matters applicable for specific types of small organi-  
14 zations in addition to matters applicable to all small  
15 organizations.

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

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

21           (B) small organizations, insurers of risks  
22 related to cybersecurity, State governments, cy-  
23 bersecurity and information technology compa-  
24 nies that work with small organizations, and

1 academic and Federal and non-Federal experts  
2 in cybersecurity.

3 (e) PERIODIC CENSUS ON STATE OF CYBERSECURITY  
4 OF SMALL BUSINESSES.—

5 (1) IN GENERAL.—Not later than 1 year after  
6 the date of enactment of this Act and not less fre-  
7 quently than every 24 months thereafter for not  
8 more than 10 years, the Administrator shall submit  
9 to Congress and make publicly available data on the  
10 state of cybersecurity of small businesses, includ-  
11 ing—

12 (A) adoption of the cybersecurity guidance  
13 among small businesses;

14 (B) the most significant and widespread  
15 cybersecurity threats facing small businesses;

16 (C) the amount small businesses spend on  
17 cybersecurity products and services; and

18 (D) the personnel small businesses dedi-  
19 cate to cybersecurity (including the amount of  
20 total personnel time, whether by employees or  
21 contractors, dedicated to cybersecurity efforts).

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

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

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

6                   (B) small businesses, insurers of risks re-  
7 lated to cybersecurity, cybersecurity and infor-  
8 mation technology companies that work with  
9 small businesses, and academic and Federal  
10 and non-Federal experts in cybersecurity.

○