I

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Improving Cybersecurity of Small Businesses, Nonprofits, and Local Governments Act''.

SEC. 2. IMPROVING CYBERSECURITY OF SMALL ENTITIES.

(a) DEFINITIONS.—In this section:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Small Business Administration.

(2) ANNUAL CYBERSECURITY REPORT; SMALL BUSINESS; SMALL ENTITY; SMALL GOVERNMENTAL JURISDICTION; SMALL ORGANIZATION.—The terms ''annual cybersecurity report'', ''small business'', ''small entity'', ''small governmental jurisdiction'', and ''small organization'' have the meanings given those terms in section 2220D of the Homeland Security Act of 2002, as added by subsection (b).

(3) CISA.—The term ''CISA'' means the Cybersecurity and Infrastructure Security Agency.

(4) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(5) SECRETARY.—The term ''Secretary'' means the Secretary of Commerce.

(b) ANNUAL REPORT.—

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

"SEC. 2220D. ANNUAL CYBERSECURITY REPORT FOR SMALL ENTITIES.

''(a) DEFINITIONS.—

''(1) ADMINISTRATION.—The term 'Administration' means the Small Business Administration.

''(2) ADMINISTRATOR.—The term 'Administrator' means the Administrator of the Administration.

''(3) ANNUAL CYBERSECURITY REPORT.—The term 'annual cybersecurity report' means the annual cybersecurity report published and promoted under subsections (b) and (c), respectively.

''(4) COMMISSION.—The term 'Commission' means the Federal Trade Commission.

''(5) ELECTRONIC DEVICE.—The term 'electronic device' means any electronic equipment that is—

''(A) used by an employee or contractor of a small entity for the purpose of performing work for the small entity;

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

''(C) capable of sending, receiving, or processing personal information.

''(6) NIST.—The term 'NIST' means the National Institute of Standards and Technology.

''(7) SMALL BUSINESS.—The term 'small business' has the meaning given the term 'small business concern' under section 3 of the Small Business Act (15 U.S.C. 632).

''(8) SMALL ENTITY.—The term 'small entity' means—

''(A) a small business;

''(B) a small governmental jurisdiction; and

''(C) a small organization.

''(9) SMALL GOVERNMENTAL JURISDICTION.—The term 'small governmental jurisdiction' means governments of cities, counties, towns, townships, villages, school districts, or special districts with a population of less than 50,000.

''(10) SMALL ORGANIZATION.—The term 'small organization' means any not-for-profit enterprise that is independently owned and operated and is not dominant in its field.

''(b) ANNUAL CYBERSECURITY REPORT.—

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

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

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

"(B) include protocols and policies to address common cybersecurity threats and risks posed by electronic devices, regardless of whether the electronic devices are—

"(i) issued by the small entity to employees and contractors of the small entity; or

"(ii) personal to the employees and contractors of the small entity; and

"(C) recommend, as practicable—

"(i) measures to improve the cybersecurity of small entities; and

"(ii) configurations and settings for some of the most commonly used software that can improve the cybersecurity of small entities.

"(2) EXISTING RECOMMENDATIONS.—The Director shall ensure that each annual cybersecurity report published under paragraph (1) incorporates—

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

"(B) the most recent version of the Cybersecurity Framework, or successor resource, maintained by NIST.

"(3) CONSIDERATION FOR SPECIFIC TYPES OF SMALL ENTITIES.—The Director may include and prioritize the development of cybersecurity recommendations, as required under paragraph (1), appropriate for specific types of small entities in addition to recommendations applicable for all small entities.

"(4) CONSULTATION.—In publishing the annual cybersecurity report under paragraph (1), the Director shall, to the degree practicable and as appropriate, consult with—

"(A) the Administrator, the Secretary of Commerce, the Commission, and the Director of NIST;

"(B) small entities, insurers, State governments, companies that work with small entities, and academic and Federal and non-Federal experts in cybersecurity; and

"(C) any other entity as determined appropriate by the Director.

"(c) PROMOTION OF ANNUAL CYBERSECURITY REPORT FOR SMALL BUSINESSES.—

"(1) PUBLICATION.—The annual cybersecurity report, and previous versions of the report as appropriate, published under subsection (b)(1) shall be—

"(A) made available, prominently and free of charge, on the public website of the Agency; and

"(B) linked to from relevant portions of the websites of the Administration and the Minority Business Development Agency, as determined by the Administrator and the Director of the Minority Business Development Agency, respectively.

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

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

nority Business Development Agency shall make available to employees of small entities voluntary training and technical assistance on how to implement the recommendations of the annual cybersecurity report.''.

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

''Sec. 2220D. Annual cybersecurity report for small entities.''.

(c) REPORT TO CONGRESS.—

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

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

(A) identify barriers or challenges for small entities in purchasing or acquiring classes of products and services that promote the cybersecurity of small entities;

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

(C) estimate the costs and benefits of policies that promote the cybersecurity of small entities, including—

(i) tax breaks;

(ii) grants and subsidies; and

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

(D) describe evidence-based cybersecurity controls and policies that improve the cybersecurity of small entities;

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

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

(3) SPECIFIC SECTORS OF SMALL ENTITIES.—In preparing the report required under paragraph (1), the Secretary may include matters applicable for

specific sectors of small entities in addition to matters applicable to all small entities.

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

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

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

(d) 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 10 years, the Administrator shall submit to Congress and make publicly available data on the state of cybersecurity of small businesses, including, to the extent practicable—

(A) adoption of the cybersecurity recommendations from the annual cybersecurity report among small businesses;

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

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

(D) the personnel small businesses dedicate to cybersecurity, including the amount of total personnel time, whether by employees or contractors, dedicated to cybersecurity efforts.

(2) VOLUNTARY PARTICIPATION.—In carrying out paragraph (1), the Administrator shall collect data from small businesses that participate on a voluntary basis.

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

(4) CONSULTATION.—In preparing to collect the data required under paragraph (1), the Administrator shall consult with—

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

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

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

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

○