Calendar No. 573

117TH CONGRESS
2d Session

SENATE

REPORT
117–217

IMPROVING CYBERSECURITY OF SMALL ORGANIZATIONS ACT OF 2021

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2483

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.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
39–010 WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	ROB PORTMAN, Ohio
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	RAND PAUL, Kentucky
JACKY ROSEN, Nevada	JAMES LANKFORD, Oklahoma
ALEX PADILLA, California	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
	JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
CARA G. MUMFORD, *Minority Director of Governmental Affairs*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 573

117TH CONGRESS
2d Session

SENATE

REPORT
117–217

IMPROVING CYBERSECURITY OF SMALL ORGANIZATIONS ACT OF 2021

DECEMBER 5, 2022.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 2483]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2483) to require the Director of the Cybersecurity and Infrastructure Security Agency to establish cybersecurity guidance for small organizations, and for other purposes, having considered the same, reports favorably thereon with amendment, in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS

I. PURPOSE AND SUMMARY

S. 2483, the *Improving Cybersecurity of Small Organizations Act of 2021*, directs the Director of the Cybersecurity and Infrastructure Security Agency (CISA) to publish an annual report that documents and promotes evidence-based cybersecurity policies and controls for small organizations—defined as small businesses, nonprofits, and local governments. The bill also requires CISA, the Small Business Administration and the Minority Business Develop-

ment Agency to offer voluntary training and technical assistance to small organizations on how to implement the recommendations of the annual cybersecurity report.

Additionally, S. 2483 directs the Secretary of Commerce to submit to Congress an annual report describing methods to incentivize small entities to improve their cybersecurity through the adoption of policies, controls, and classes of products and services that have been demonstrated to reduce cybersecurity risks. The bill also requires the Small Business Administration to report on the state of small business cybersecurity in a biannual report to Congress.

II. Background and Need for the Legislation

According to the Federal Bureau of Investigation's 2020 Internet Crime Report, the cost of cybercrimes reached $4.1 billion in 2020.[1] Many small organizations have become targets because they have valuable information and typically lack the security infrastructure of larger organizations. In 2020, 70% of ransomware incidents were at companies with fewer than 1,000 employees.[2] As of 2020, there were 31.7 million small businesses in the United States, with 6 million having paid employees.[3]

This bill is intended to address the cybersecurity challenges that became apparent when small businesses, small nonprofits, and small government jurisdictions had many of their employees working remotely at the start of the COVID–19 pandemic. Many of these small organizations were unprepared for telework and the surge of ransomware and other cyberattacks that came with the pandemic. In 2021, only 28% of small businesses said that they had a response plan in place in the event of a cyberattack.[4] Without proper resources to protect themselves, cyberattacks will continue to devastate small organizations.

Cyberattacks have evolved in sophistication and increasingly target small organizations. Between 2020 and 2021, data breaches at small businesses increased 152%, compared to a 75% increase at larger organizations.[5] This bill aims to make more tailored resources available to small organizations, small businesses, small government jurisdictions, and to support those organizations' ability to utilize those resources. In doing so, the bill will expand cybersecurity hygiene among smaller organizations that are not necessarily able to maintain resources dedicated to cybersecurity.

III. Legislative History

Senator Rosen (D–NV) introduced S. 2483, the *Improving the Cybersecurity of Small Organizations Act of 2021*, on July 27, 2021,

---

[1] Federal Bureau of Investigation, *FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID–19 Scam Statistics* (2021) (https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics).

[2] Coveware, *Why Small and Medium-Sized Professional Service Firms Are a Big Target for Ransomware Attacks* (2021) (https://www.coveware.com/blog/2020/11/30/why-small-professional-service-firms-are-ransomware-targets).

[3] Small Business Administration, *Frequently Asked Questions* (2020) (https://cdn.advocacy.sba.gov/wp-content/uploads/2020/11/05122043/Small-Business-FAQ 2020.pdf).

[4] Eric Rosenbaum, *Main Street overconfidence: America's small businesses aren't worried about hacking* (2021) (https://www.cnbc.com/2021/08/10/main-street-overconfidence-small-businesses-dont-worry-about-hacking.html).

[5] Riskrecon, *Small Business, Mighty Attack Surface* (2022) (https://blog.riskrecon.com/company/media-coverage/small-business-mighty-attack-surface).

with Senator Cornyn (R–TX). The bill was referred to the Committee on Homeland Security and Governmental Affairs. Senators Ossoff (D–GA) and Hassan (D–NH) later joined as co-sponsors on November 1, 2021 and January 31, 2022, respectively.

The Committee considered S. 2483 at a business meeting on February 2, 2022. During the business meeting, Senator Rosen offered a substitute amendment to require the CISA Director to publish an annual cybersecurity report, rather than issue guidance. The Rosen substitute amendment also included changes to require the CISA Director, the Administrator of the Small Business Administration, and the Director of the Minority Business Development Agency to make available voluntary cybersecurity training to small entities. The Rosen substitute amendment, as modified, was adopted by voice vote *en bloc* with Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Lankford, Scott, and Hawley present.

The bill, as amended, was ordered reported favorably by voice vote *en bloc*. Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Lankford, Scott, and Hawley were present for the vote.

IV. Section-by-Section Analysis of the Bill, as Reported

Sec. 1. Short title

The title of the bill is the "Improving Cybersecurity of Small Businesses, Nonprofits, and Local Governments Act of 2021."

Sec. 2. Improving Cybersecurity of Small Entities

Subsection a defines "Administrator," "Cybersecurity Report," "Small Business," "Small Entity," "Small Governmental Jurisdiction," "Small Organization," "CISA," "Commission," and "Secretary."

Subsection (b) amends Subtitle A of title XXII of the Homeland Security Act of 2002 by adding at the end the following:

"Sec. 2220D. Annual Cybersecurity Report for Small Entities."

(a) Definitions

Defines "Administration," "Administrator," "Annual Cybersecurity Report," "Commission," "Electronic Device," "NIST," "Small Business," "Small Entity," "Small Governmental Jurisdiction," and "Small Organization." Definitions are repeated because the legislation uses terms that are both in freestanding and amendatory language.

(b) Annual Cybersecurity Report

Directs the Director of CISA to publish an annual report a report for small entities that documents and promotes evidence-based cybersecurity policies and controls for use by small entities. The annual report shall incorporate existing recommendations, including cybersecurity resources developed by NIST and the most recent version of the Cybersecurity Framework maintained by NIST. In preparing the report, the Director of CISA shall consult with other relevant agencies, as well as small entities, insurers, State governments, companies that work with small entities, and academic, Federal and non-Federal experts in cybersecurity.

(c) Promotion of Annual Cybersecurity Report

Requires the annual cybersecurity report to be made available on CISA's website and promoted by the Director of CISA, Administrator of the Small Business Administration, and Secretary of Commerce.

(d) Training and Technical Assistance

Directs CISA, the Small Business Administration and the Minority Business Development Agency to offer to small entities voluntary training and technical assistance on how to implement the recommendations of the annual cybersecurity report.

Subsection (c) directs the Secretary of Commerce to submit to Congress an annual report for 10 years describing methods to incentivize small entities to improve their cybersecurity including through the adoption of policies, controls, and products and services that have been demonstrated to reduce cybersecurity risk.

Subsection (d) requires the Administrator of the Small Business Administration to report every two years on the state of small business cybersecurity, and submit that data to Congress. In carrying out the census, the Administrator shall collect data from small businesses on a voluntary basis and will ensure that any publicly available data is anonymized and does not reveal personally identifiable information.

Subsection (e) provides a rule of construction to clarify that the bill does not provide additional regulatory to CISA.

V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. Congressional Budget Office Cost Estimate

U.S. Congress,
Congressional Budget Office,
Washington, DC, May 13, 2022.

Hon. Gary C. Peters,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

Dear Mr. Chairman: The Congressional Budget Office has prepared the enclosed cost estimate for S. 2483, the Improving Cybersecurity of Small Businesses, Nonprofits, and Local Governments Act of 2021.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

Phillip L. Swagel,
Director.

Enclosure.

S. 2483, Improving Cybersecurity of Small Businesses, Nonprofits, and Local Governments Act of 2021

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on February 2, 2022

By Fiscal Year, Millions of Dollars	2022	2022-2027	2022-2032
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	10	not estimated

Statutory pay-as-you-go procedures apply?	No	**Mandate Effects**	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2032?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

S. 2483 would require the Cybersecurity and Infrastructure Security Agency (CISA) to offer cybersecurity training to employees of small businesses. The bill also would require CISA and the Small Business Administration to provide the Congress with recommendations for ways to reduce cyber vulnerabilities in the information networks of small businesses.

Using information from CISA, CBO anticipates that the agency would need five full-time employees to create and manage the new training program. CBO estimates that costs for staff salaries and website development would total $2 million annually. Accounting for the time needed to hire new employees and develop the training, CBO estimates that implementing the bill would cost $10 million over the 2022–2027 period; such spending would be subject to the availability of appropriated funds.

The CBO staff contacts for this estimate are Aldo Prosperi (Department of Homeland Security) and David Hughes (Small Business Administration). The estimate was reviewed by Leo Lex, Deputy Director of Budget Analysis.

VII. Changes in Existing Law Made by the Bill, as Reported

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

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' in 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; 132 Stat. 2444); and

(B) the most recent version of the Cybersecurity Framework, or a 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 Minority 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.

○