118TH CONGRESS
1ST SESSION

S. 2740

To help small businesses prepare for and combat cybersecurity threats, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 7, 2023

Mr. RISCH (for himself, Mrs. SHAHEEN, Mr. CRAPO, and Ms. CORTEZ MASTO) introduced the following bill; which was read twice and referred to the Committee on Small Business and Entrepreneurship

---

A BILL

To help small businesses prepare for and combat cybersecurity threats, 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 ''Small Business Cyber Resiliency Act''.

SEC. 2. SMALL BUSINESS CYBERSECURITY.

(a) IN GENERAL.—The Small Business Act (15 U.S.C. 631 et seq.) is amended—

(1) by redesignating section 49 (15 U.S.C. 631 note) as section 52; and

(2) by inserting after section 48 (15 U.S.C. 657u) the following:

"SEC. 49. SMALL BUSINESS CYBERSECURITY.

"(a) DEFINITIONS.—In this section:

"(1) CYBERSECURITY RISK; CYBER THREAT INDICATOR; DEFENSIVE MEASURE; INCIDENT.—The terms 'cybersecurity risk', 'cyber threat indicator', 'defense measure', and 'incident' have the meanings given those terms in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

"(2) RESOURCE PARTNER.—The term 'resource partner' means—

"(A) a small business development center;

"(B) a women's business center described in section 29; and

"(C) a chapter of the Service Corps of Retired Executives described in section 8(a)(1)(A).

"(b) INTERAGENCY AGREEMENT.—The Administration shall enter into an interagency agreement with the Cybersecurity and Infrastructure Security Agency to collaborate and increase information sharing with the Administration to improve cybersecurity resources and defenses for small business concerns, including cybersecurity products tailored to the needs of small business concerns.

''(c) ASSISTANCE THROUGH RESOURCE PARTNERS.—

''(1) IN GENERAL.—The Department of Homeland Security, and any other Federal agency in coordination with the Department of Homeland Security, shall leverage resource partners to provide assistance to small business concerns with cybersecurity tools, such as the Cyber Security Evaluation Tool and the Cyber Resilience Review, and by disseminating information relating to cybersecurity risks and other homeland security matters to help small business concerns in developing or enhancing cybersecurity infrastructure, awareness of cyber threat indicators, cybersecurity incident response planning, and cyber training programs for employees.

''(2) ANNUAL PUBLICATION.—Not later than 1 year after the date of enactment of the Small Business Cyber Resiliency Act and annually thereafter, the Administrator shall publish on the website of the Administration the number of small business concerns that resource partners assisted in providing assistance described in paragraph (1) during the year covered by the publication.

''(d) CENTRAL SMALL BUSINESS CYBERSECURITY ASSISTANCE UNIT.—

''(1) ESTABLISHMENT.—The Administrator, in coordination with the Secretary of Commerce, and in consultation with the Secretary of Homeland Security and the Attorney General, shall establish a central small business cybersecurity assistance unit within the Administration, which shall serve as a central clearinghouse for cybersecurity resources for small business concerns across the Federal Government, such as those developed by the Department of Homeland Security.

''(2) DUTIES.—The central small business cybersecurity assistance unit established under paragraph (1) shall—

''(A) coordinate internal cybersecurity efforts within the Administration to reduce duplication of effort and resources;

''(B) establish and maintain a publicly available website that is a clearinghouse of cybersecurity information for small business concerns, including information on—

''(i) how to find guidance material on best cyber hygiene practices;

"(ii) where to report cybersecurity breaches or incidents;

"(iii) how to respond to cybersecurity breaches or incidents;

"(iv) the cybersecurity efforts of the Administration;

"(v) how to contact the certified employees described in section 21(o); and

"(vi) standard incident response procedures for leading cyber crimes;

"(C) work with the certified employees described in section 21(o) to provide cybersecurity assistance to small business concerns;

"(D) coordinate with the Department of Homeland Security and any other Federal agency as the Administrator determines appropriate to identify and disseminate cybersecurity information and resources to small business concerns in a form that is accessible and actionable by small business concerns;

"(E) redirect small business cybersecurity inquiries, such as reporting of cyber threat indicators and defensive measures, to the appropriate Federal agencies;

''(F) coordinate with the National Institute of Standards and Technology to identify and disseminate information to small business concerns on the most cost-effective methods for implementing elements of the cybersecurity framework of the National Institute of Standards and Technology applicable to improving the cybersecurity posture of small business concerns;

''(G) coordinate with the Department of Defense to identify and disseminate information to small business concerns on satisfying the applicable requirements of the Cybersecurity Maturity Model Certification of the Department of Defense or any other successor cybersecurity requirements as established by the Department of Defense; and

''(H) seek input from the Office of Advocacy of the Administration to identify any policies or procedures adopted by any department, agency, or instrumentality of the Federal Government that will hamper the improvement of the cybersecurity posture of those small business concerns.

''(3) ENHANCED CYBERSECURITY PROTECTIONS FOR SMALL BUSINESSES.—

"(A) IN GENERAL.—Notwithstanding any other provision of law, no cause of action shall lie or be maintained in any court against any small business concern, and such action shall be promptly dismissed, if such action is related to or arises out of—

"(i) any activity authorized under this paragraph or the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.); or

"(ii) any action or inaction in response to any cyber threat indicator, defensive measure, or other information shared or received pursuant to this paragraph or the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.).

"(B) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to affect the applicability or merits of any defense, motion, or argument in any cause of action in a court brought against an entity that is not a small business concern.

"(e) REPORT.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of the Small Business Cyber Resiliency Act, and every year thereafter, the Administrator and the head of each Federal agency that collects or shares information under this section shall submit to the Committee on Small Business and Entrepreneurship of the Senate and the Committee on Small Business of the House of Representatives a joint report on actions taken by the Administration and relevant Federal agencies to protect personally identifiable information, business identifiable information, sensitive financial information, and cybersecurity information received by those Federal agencies as a result of the requirements under this section.

''(2) FORM.—Each report required under paragraph (1) shall be unclassified, but may include a classified annex.''.

(b) PROHIBITION ON NEW APPROPRIATIONS.—

(1) IN GENERAL.—No additional funds are authorized to be appropriated to carry out this section and the amendments made by this section.

(2) EXISTING FUNDING.—This section and the amendments made by this section shall be carried out using amounts made available to the Small Busi-

ness Administration under the heading ''Entrepreneurial Development Programs''.

(c) IMPLEMENTATION.—Not later than 180 days after the date of enactment of this Act, the Administrator of the Small Business Administration shall implement this section and the amendments made by this section.

SEC. 3. STUDY AND REPORT ON CYBERSECURITY RISKS OF SMALL BUSINESSES.

(a) DEFINITIONS.—In this section:

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

(2) APPROPRIATE COMMITTEES OF CONGRESS.—The term ''appropriate committees of Congress'' means—

(A) the Committee on Small Business and Entrepreneurship of the Senate;

(B) the Committee on Homeland Security and Governmental Affairs of the Senate;

(C) the Committee on Small Business of the House of Representatives; and

(D) the Committee on Homeland Security of the House of Representatives.

(3) CYBERSECURITY RISK.—The term ''cybersecurity risk'' has the meaning given the term in sec-

tion 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(4) INFORMATION SYSTEM.—The term ''information system'' has the meaning given the term in section 3502 of title 44, United States Code.

(5) RURAL AREA.—The term ''rural area'' means any county or other political subdivision of a State, the District of Columbia, or a territory or possession of the United States that is designated as a rural area by the Bureau of the Census.

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

(b) STUDY AND REPORT.—Not later than 1 year after the date of enactment of this Act, the Chief Counsel for Advocacy of the Administration and the Comptroller General of the United States shall—

(1) conduct a joint study assessing the impact of small business concerns turning to online marketplaces as a result of shutdowns imposed by the COVID–19 pandemic, specifically in regards to the cybersecurity of those small business concerns; and

(2) submit to the appropriate committees of Congress and make publicly available a report on—

(A) how identified cybersecurity risks specifically impact small business concerns that established an online presence during the period beginning on February 1, 2020, and ending on December 31, 2021;

(B) the challenges that the small business concerns described in subparagraph (A) face in—

(i) securing updated information systems;

(ii) implementing cybersecurity protocols; and

(iii) responding to data breaches or cyber attacks;

(C) the Federal resources that the small business concerns described in subparagraph (A) used in establishing the online presence described in that paragraph;

(D) as of the date of the report, the cybersecurity status of the small business concerns described in subparagraph (A) based on a representative sample of those small business concerns;

(E) how the Department of Homeland Security and the Administration can improve their

existing partnership to better train small business concerns regarding cybersecurity threats; and

(F) as of the date of the report—

(i) the frequency of each type of cyber attack suffered by small business concerns described in subparagraph (A); and

(ii) an estimated average cost to those small business concerns of each type of cyber attack.

○