I

115TH CONGRESS
1ST SESSION

H. R. 4668

To amend the Small Business Act to provide for the establishment of an enhanced cybersecurity assistance and protections for small businesses, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 18, 2017

Mr. CHABOT (for himself and Ms. VELÁZQUEZ) introduced the following bill; which was referred to the Committee on Small Business

---

A BILL

To amend the Small Business Act to provide for the establishment of an enhanced cybersecurity assistance and protections for small businesses, 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 Advanced Cybersecurity Enhancements Act of 2017''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) Small businesses represent more than 97 percent of total businesses in the United States and

make up an essential part of the supply chain to some of the largest companies, many of which are in critical infrastructure sectors, from financial and transportation organizations to power, water, and healthcare suppliers.

(2) Many small businesses do not have dedicated information technology (''IT'') departments and must outsource IT functions or assign these duties to an employee as a secondary function.

(3) The Internet Crime Complaint Center within the United States Department of Justice recorded 298,728 cybersecurity-related complaints in its 2016 report.

(4) There has been steady increases of cybersecurity-related complaints year over year since the year 2000, totaling 3,762,348.

(5) Seventy-one percent of cyber attacks occurred in businesses with fewer than 100 employees.

(6) Only 14 percent of small- and medium-sized businesses believe they have the ability to effectively mitigate cyber risks and vulnerabilities.

(7) Small businesses risk theft and manipulation of sensitive data if they lack adequate cybersecurity measures.

(8) The Better Business Bureau found that half of small businesses could remain profitable for only one month if they lost essential data.

(9) Cyber crime is growing rapidly and the annual costs to the global economy are estimated to reach over $2,000,000,000,000 by 2019.

(10) Cybersecurity is a global challenge where the security threat, attacks, and techniques continually evolve and no company, individual, or Federal agency is immune from these threats.

(11) Strong collaboration between the public and private sector is essential in the fight against cyber crime.

(12) There is a reluctance among small businesses to voluntarily share information with government entities, and the Federal Government should work proactively to incentivize and encourage voluntary information sharing to improve the Nation's cybersecurity posture.

SEC. 3. ENHANCED CYBERSECURITY ASSISTANCE AND PROTECTIONS FOR SMALL BUSINESSES.

Section 21(a) of the Small Business Act (15 U.S.C. 648(a)) is amended by adding at the end the following new paragraph:

''(9) SMALL BUSINESS CYBERSECURITY ASSISTANCE AND PROTECTIONS.—

''(A) ESTABLISHMENT OF SMALL BUSINESS CYBERSECURITY ASSISTANCE UNITS.—The Administrator of the Small Business Administration, in coordination with the Secretary of Commerce, and in consultation with the Secretary of Homeland Security and the Attorney General, shall establish—

''(i) in the Administration, a central small business cybersecurity assistance unit; and

''(ii) within each small business development center, a regional small business cybersecurity assistance unit.

''(B) DUTIES OF THE CENTRAL SMALL BUSINESS CYBERSECURITY ASSISTANCE UNIT.—

''(i) IN GENERAL.—The central small business cybersecurity assistance unit established under subparagraph (A)(i) shall serve as the primary interface for small business concerns to receive and share cyber threat indicators and defensive measures with the Federal Government.

"(ii) USE OF CAPABILITY AND PROCESSES.—The central small business cybersecurity assistance unit shall use the capability and process certified pursuant to section 105(c)(2)(A) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1504(c)(2)(A)) to receive cyber threat indicators or defensive measures from small business concerns.

"(iii) APPLICATION OF CISA.—A small business concern that receives or shares cyber threat indicators and defensive measures with the Federal Government through the central small business cybersecurity assistance unit established under subparagraph (A)(i), or with any appropriate entity pursuant to section 103(c) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1503(c)), shall receive the protections and exemptions provided in such Act and this paragraph.

"(C) RELATION TO NCCIC.—

"(i) CENTRAL SMALL BUSINESS CYBERSECURITY ASSISTANCE UNIT.—The central small business cybersecurity assist-

ance unit established under subparagraph (A)(i) shall be collocated with the national cybersecurity and communications integration center.

"(ii) ACCESS TO INFORMATION.—The national cybersecurity and communications integration center shall have access to all cyber threat indicators or defensive measures shared with the central small cybersecurity assistance unit established under subparagraph (A)(i) through the use of the capability and process described in subparagraph (B)(ii).

"(D) CYBERSECURITY ASSISTANCE FOR SMALL BUSINESSES.—The central small business cybersecurity assistance unit established under subparagraph (A)(i) shall—

"(i) work with each regional small business cybersecurity assistance unit established under subparagraph (A)(ii) to provide cybersecurity assistance to small business concerns;

"(ii) leverage resources from the Administration, the Department of Commerce, the Department of Homeland Secu-

rity, the Department of Justice, the Department of the Treasury, the Department of State, and any other Federal department or agency the Administrator determines appropriate, in order to help improve the cybersecurity posture of small business concerns;

''(iii) coordinate with the Department of Homeland Security to identify and disseminate information to small business concerns in a form that is accessible and actionable by small business concerns;

''(iv) 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;

''(v) seek input from the Office of Advocacy of the Administration to ensure that any policies or procedures adopted by

any department, agency, or instrumentality of the Federal Government do not unduly add regulatory burdens to small business concerns in a manner that will hamper the improvement of the cybersecurity posture of such small business concerns; and

''(vi) leverage resources and relationships with representatives and entities involved in the national cybersecurity and communications integration center to publicize the capacity of the Federal Government to assist small business concerns in improving cybersecurity practices.

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

''(i) 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 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.).

''(ii) APPLICATION.—The exception provided in section 105(d)(5)(D)(ii)(I) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1504(d)(5)(D)(ii)(I)) shall not apply to any cyber threat indicator or defensive measure shared or received by small business concerns pursuant to this paragraph or the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.).

''(F) DEFINITIONS.—In this paragraph:

''(i) CISA DEFINITIONS.—The terms 'cyber threat indicator' and 'defensive measure' have the meanings given such terms in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

"(ii) NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.—The term 'national cybersecurity and communications integration center' means the national cybersecurity and communications integration center established under section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148).".

SEC. 4. PROHIBITION ON NEW APPROPRIATIONS.

No additional funds are authorized to be appropriated to carry out this Act and the amendments made by this Act, and this Act and such amendments shall be carried out using amounts otherwise made available for such purposes.

○