

115TH CONGRESS
2D SESSION

S. 2735

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 SENATE OF THE UNITED STATES

APRIL 24, 2018

Mr. RISCH (for himself and Mr. PETERS) introduced the following bill; which was read twice and referred to the Committee on Small Business and Entrepreneurship

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.

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 “Small Business Ad-
5 vanced Cybersecurity Enhancements Act of 2018”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

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

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

6 (2) Many small businesses do not have dedi-
7 cated information technology (“IT”) departments
8 and must outsource IT functions or assign these du-
9 ties to an employee as a secondary function.

10 (3) The Internet Crime Complaint Center with-
11 in the Department of Justice recorded 298,728 cy-
12 bersecurity-related complaints in its 2016 report.

13 (4) There has been steady increases of cyberse-
14 curity-related complaints year over year since the
15 year 2000, totaling 3,762,348.

16 (5) Seventy-one percent of cyber attacks oc-
17 curred in businesses with fewer than 100 employees.

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

21 (7) Small businesses risk theft and manipula-
22 tion of sensitive data if they lack adequate cyberse-
23 curity measures.

1 (8) The Better Business Bureau found that
2 half of small businesses could remain profitable for
3 only 1 month if they lost essential data.

4 (9) Cyber crime is growing rapidly and the an-
5 nual costs to the global economy are estimated to
6 reach over \$2,000,000,000,000 by 2019.

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

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

14 (12) There is a reluctance among small busi-
15 nesses to voluntarily share information with govern-
16 ment entities, and the Federal Government should
17 work proactively to incentivize and encourage vol-
18 untary information sharing to improve the cyberse-
19 curity posture of the United States.

20 **SEC. 3. ENHANCED CYBERSECURITY ASSISTANCE AND PRO-**
21 **TECTIONS FOR SMALL BUSINESSES.**

22 Section 21(a) of the Small Business Act (15 U.S.C.
23 648(a)) is amended by adding at the end the following:

24 “(9) SMALL BUSINESS CYBERSECURITY ASSIST-
25 ANCE AND PROTECTIONS.—

1 “(A) ESTABLISHMENT OF SMALL BUSI-
2 NESS CYBERSECURITY ASSISTANCE UNITS.—
3 The Administrator, in coordination with the
4 Secretary of Commerce, and in consultation
5 with the Secretary of Homeland Security and
6 the Attorney General, shall establish—

7 “(i) in the Administration, a central
8 small business cybersecurity assistance
9 unit; and

10 “(ii) within each small business devel-
11 opment center, a regional small business
12 cybersecurity assistance unit.

13 “(B) DUTIES OF THE CENTRAL SMALL
14 BUSINESS CYBERSECURITY ASSISTANCE UNIT.—

15 “(i) IN GENERAL.—The central small
16 business cybersecurity assistance unit es-
17 tablished under subparagraph (A)(i) shall
18 serve as the primary interface for small
19 business concerns to receive and share
20 cyber threat indicators and defensive meas-
21 ures with the Federal Government.

22 “(ii) USE OF CAPABILITY AND PROC-
23 ESS.—The central small business cyberse-
24 curity assistance unit shall use the capa-
25 bility and process certified pursuant to sec-

1 tion 105(c)(2)(A) of the Cybersecurity In-
2 formation Sharing Act of 2015 (6 U.S.C.
3 1504(c)(2)(A)) to receive cyber threat indi-
4 cators or defensive measures from small
5 business concerns.

6 “(iii) APPLICATION OF CISA.—A small
7 business concern that receives or shares
8 cyber threat indicators and defensive meas-
9 ures with the Federal Government through
10 the central small business cybersecurity as-
11 sistance unit established under subpara-
12 graph (A)(i), or with any appropriate enti-
13 ty pursuant to section 104(c) of the Cyber-
14 security Information Sharing Act of 2015
15 (6 U.S.C. 1503(c)), shall receive the pro-
16 tections and exemptions provided in such
17 Act and this paragraph.

18 “(C) RELATION TO NCCIC.—

19 “(i) CENTRAL SMALL BUSINESS CY-
20 BERSECURITY ASSISTANCE UNIT.—The
21 central small business cybersecurity assist-
22 ance unit established under subparagraph
23 (A)(i) shall be collocated with the national
24 cybersecurity and communications integra-
25 tion center.

1 “(ii) ACCESS TO INFORMATION.—The
2 national cybersecurity and communications
3 integration center shall have access to all
4 cyber threat indicators or defensive meas-
5 ures shared with the central small cyberse-
6 curity assistance unit established under
7 subparagraph (A)(i) through the use of the
8 capability and process described in sub-
9 paragraph (B)(ii).

10 “(D) CYBERSECURITY ASSISTANCE FOR
11 SMALL BUSINESSES.—The central small busi-
12 ness cybersecurity assistance unit established
13 under subparagraph (A)(i) shall—

14 “(i) work with each regional small
15 business cybersecurity assistance unit es-
16 tablished under subparagraph (A)(ii) to
17 provide cybersecurity assistance to small
18 business concerns;

19 “(ii) leverage resources from the Ad-
20 ministration, the Department of Com-
21 merce, the Department of Homeland Secu-
22 rity, the Department of Justice, the De-
23 partment of the Treasury, the Department
24 of State, and any other Federal depart-
25 ment or agency the Administrator deter-

1 mines appropriate, in order to help im-
2 prove the cybersecurity posture of small
3 business concerns;

4 “(iii) coordinate with the Department
5 of Homeland Security to identify and dis-
6 seminate information to small business
7 concerns in a form that is accessible and
8 actionable by small business concerns;

9 “(iv) coordinate with the National In-
10 stitute of Standards and Technology to
11 identify and disseminate information to
12 small business concerns on the most cost-
13 effective methods for implementing ele-
14 ments of the cybersecurity framework of
15 the National Institute of Standards and
16 Technology applicable to improving the cy-
17 bersecurity posture of small business con-
18 cerns;

19 “(v) seek input from the Office of Ad-
20 vocacy of the Administration to ensure
21 that any policies or procedures adopted by
22 any department, agency, or instrumentality
23 of the Federal Government do not unduly
24 add regulatory burdens to small business
25 concerns in a manner that will hamper the

1 improvement of the cybersecurity posture
2 of those small business concerns; and

3 “(vi) leverage resources and relation-
4 ships with representatives and entities in-
5 volved in the national cybersecurity and
6 communications integration center to pub-
7 licize the capacity of the Federal Govern-
8 ment to assist small business concerns in
9 improving cybersecurity practices.

10 “(E) ENHANCED CYBERSECURITY PROTEC-
11 TIONS FOR SMALL BUSINESSES.—

12 “(i) IN GENERAL.—Notwithstanding
13 any other provision of law, no cause of ac-
14 tion shall lie or be maintained in any court
15 against any small business concern, and
16 such action shall be promptly dismissed, if
17 such action is related to or arises out of—

18 “(I) any activity authorized
19 under this paragraph or the Cyberse-
20 curity Information Sharing Act of
21 2015 (6 U.S.C. 1501 et seq.); or

22 “(II) any action or inaction in re-
23 sponse to any cyber threat indicator,
24 defensive measure, or other informa-
25 tion shared or received pursuant to

1 this paragraph or the Cybersecurity
2 Information Sharing Act of 2015 (6
3 U.S.C. 1501 et seq.).

4 “(ii) APPLICATION.—The exception
5 provided in section 105(d)(5)(D)(ii)(I) of
6 the Cybersecurity Information Sharing Act
7 of 2015 (6 U.S.C. 1504(d)(5)(D)(ii)(I))
8 shall not apply to any cyber threat indi-
9 cator or defensive measure shared or re-
10 ceived by small business concerns pursuant
11 to this paragraph or the Cybersecurity In-
12 formation Sharing Act of 2015 (6 U.S.C.
13 1501 et seq.).

14 “(iii) RULE OF CONSTRUCTION.—
15 Nothing in this subparagraph shall be con-
16 strued to affect the applicability or merits
17 of any defense, motion, or argument in any
18 cause of action in a court brought against
19 an entity that is not a small business con-
20 cern.

21 “(F) DEFINITIONS.—In this paragraph:

22 “(i) CISA DEFINITIONS.—The terms
23 ‘cyber threat indicator’ and ‘defensive
24 measure’ have the meanings given those
25 terms in section 102 of the Cybersecurity

1 Information Sharing Act of 2015 (6
2 U.S.C. 1501).

3 “(ii) NATIONAL CYBERSECURITY AND
4 COMMUNICATIONS INTEGRATION CEN-
5 TER.—The term ‘national cybersecurity
6 and communications integration center’
7 means the national cybersecurity and com-
8 munications integration center established
9 under section 227 of the Homeland Secu-
10 rity Act of 2002 (6 U.S.C. 148).”.

11 **SEC. 4. PROHIBITION ON NEW APPROPRIATIONS.**

12 (a) IN GENERAL.—No additional funds are author-
13 ized to be appropriated to carry out this Act and the
14 amendments made by this Act.

15 (b) EXISTING FUNDING.—This Act and the amend-
16 ments made by this Act shall be carried out using amounts
17 made available under section 21(a)(4)(C)(viii) of the Small
18 Business Act (15 U.S.C. 648(a)(4)(C)(viii)).

19 (c) TECHNICAL AND CONFORMING AMENDMENT.—
20 Section 21(a)(4)(C)(viii) of the Small Business Act (15
21 U.S.C. 648(a)(4)(C)(viii)) is amended to read as follows:

22 “(viii) LIMITATION.—

23 “(I) CYBERSECURITY ASSIST-
24 ANCE.—From the funds appropriated
25 pursuant to clause (vii), the Adminis-

1 tration shall reserve not less than
2 \$1,000,000 in each fiscal year to de-
3 velop cybersecurity assistance units at
4 small business development centers
5 under paragraph (9).

6 “(II) PORTABLE ASSISTANCE.—

7 “(aa) IN GENERAL.—Any
8 funds appropriated pursuant to
9 clause (vii) that are remaining
10 after reserving amounts under
11 subclause (I) may be used for
12 portable assistance for startup
13 and sustainability non-matching
14 grant programs to be conducted
15 by eligible small business develop-
16 ment centers in communities that
17 are economically challenged as a
18 result of a business or govern-
19 ment facility down sizing or clos-
20 ing, which has resulted in the
21 loss of jobs or small business in-
22 stability.

23 “(bb) GRANT AMOUNT AND
24 USE.—A non-matching grant
25 under this clause shall not exceed

1 \$100,000, and shall be used for
2 small business development cen-
3 ter personnel expenses and re-
4 lated small business programs
5 and services.”.

○