

115TH CONGRESS
2D SESSION

S. 2666

To improve assistance provided by the Hollings Manufacturing Extension Partnership to small manufacturers in the defense industrial supply chain on matters relating to cybersecurity, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 12, 2018

Mr. COONS (for himself, Mr. GRAHAM, and Mrs. GILLIBRAND) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To improve assistance provided by the Hollings Manufacturing Extension Partnership to small manufacturers in the defense industrial supply chain on matters relating to cybersecurity, 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 “Enhance Cybersecurity
5 for Small Manufacturers Act of 2018”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

1 (1) According to the Bureau of Labor Statis-
2 tics, there are more than 347,000 manufacturing es-
3 tablishments in the United States, of which 72 per-
4 cent have fewer than 20 employees and 99 percent
5 have fewer than 500 employees.

6 (2) Independent studies from the National De-
7 fense Industry Association, the Defense Science
8 Board, the Alliance for Manufacturing Foresight,
9 and the McKinsey Global Institute have high-
10 lighted—

11 (A) the centrality of small manufacturers
12 to United States manufacturing supply chains
13 for domestic economic growth;

14 (B) the vulnerability of such manufactur-
15 ers to the defense industrial base for national
16 security; and

17 (C) the vulnerability of such manufacturers
18 to cybersecurity threats and breaches.

19 (3) As of December 31, 2017, Department of
20 Defense suppliers must comply with new, tougher
21 cybersecurity requirements to ensure adequate secu-
22 rity to protect controlled unclassified information
23 relevant to defense manufacturing supply chains.
24 The requirements call for defense suppliers to imple-
25 ment and create a plan of action to respond to the

1 guidance developed by the National Institute of
2 Standards and Technology.

3 (4) The Department of Commerce has found
4 significant cybersecurity vulnerability of small manu-
5 facturers. A survey of 9,000 contract facilities docu-
6 mented that 6,650 small facilities lagged behind me-
7 dium and large firms across a broad range of 20 cy-
8 bersecurity indicators. For several indicators, fewer
9 than half of small firms had cybersecurity measures
10 in place.

11 (5) Over the past 5 years the national network
12 of centers operating as part of the Hollings Manu-
13 facturing Extension Partnership has worked closely
14 with the Department of Defense to bolster the resil-
15 ience of the defense industrial base supply chain.
16 Since 2013, such centers have completed more than
17 2,500 projects with 1,650 companies that are sup-
18 pliers to the Department of Defense.

19 (6) In 2017, the Hollings Manufacturing Ex-
20 tension Partnership interacted with more than 1,000
21 small manufacturers on the cybersecurity require-
22 ments of the Department of Defense. This work by
23 the Hollings Manufacturing Extension Partnership
24 has revealed a significant lack of awareness of the
25 Department of Defense cybersecurity requirements

1 and a deficiency of financial and technical resources
2 required to manage cybersecurity risks. If cybersecu-
3 rity vulnerabilities remain unaddressed, defense sup-
4 ply chains face a higher likelihood of serious and ex-
5 ploitable vulnerabilities, as well as a substantial re-
6 duction in the number of suppliers compliant with
7 Department of Defense requirements, and thereby
8 ineligible to provide products and services to the De-
9 partment of Defense.

10 (7) The Hollings Manufacturing Extension
11 Partnership is well positioned to aid suppliers of the
12 Department of Defense in complying with cybersecu-
13 rity requirements of the Department to ensure ade-
14 quate security to protect controlled unclassified in-
15 formation relevant to defense manufacturing supply
16 chains.

17 **SEC. 3. ASSISTANCE FOR SMALL MANUFACTURERS IN THE**
18 **DEFENSE INDUSTRIAL SUPPLY CHAIN ON**
19 **MATTERS RELATING TO CYBERSECURITY.**

20 (a) DEFINITIONS.—In this section:

21 (1) CENTER.—The term “Center” has the
22 meaning given such term in section 25(a) of the Na-
23 tional Institute of Standards and Technology Act
24 (15 U.S.C. 278k(a)).

1 (2) DIRECTOR.—The term “Director” means
2 the Director of the National Institute of Standards
3 and Technology.

4 (3) RESOURCES.—The term “resources” means
5 guidelines, tools, best practices, standards, meth-
6 odologies, and other ways of providing information.

7 (4) SMALL BUSINESS CONCERN.—The term
8 “small business concern” means a small business
9 concern as that term is used in section 3 of the
10 Small Business Act (15 U.S.C. 632).

11 (5) SMALL MANUFACTURER.—The term “small
12 manufacturer” means a small business concern that
13 is a manufacturer.

14 (6) STATE.—The term “State” means each of
15 the several States, Territories, and possessions of
16 the United States, the District of Columbia, and the
17 Commonwealth of Puerto Rico.

18 (b) DISSEMINATION OF CYBERSECURITY RE-
19 SOURCES.—

20 (1) IN GENERAL.—The Director of the National
21 Institute of Standards and Technology, in partner-
22 ship with the Secretary of Defense and acting
23 through the Hollings Manufacturing Extension Part-
24 nership, shall take such actions as may be necessary
25 to address a widespread lack of awareness of cyber-

1 security threats among small manufacturers in the
2 defense industrial supply chain.

3 (2) NATIONAL REACH.—The Director shall en-
4 sure that efforts to increase awareness under para-
5 graph (1) are carried out in each State, by dissemi-
6 nating clear and concise resources to help reduce cy-
7 bersecurity risks faced by small manufacturers de-
8 scribed in paragraph (1).

9 (3) SECTOR FOCUS.—The Director shall carry
10 out this subsection with a focus on such industry
11 sectors as the Director considers critical, in con-
12 sultation with the Secretary of Defense.

13 (4) OUTREACH EVENTS.—Under paragraph (1),
14 the Director shall conduct outreach. Such outreach
15 may include live events with a physical presence and
16 outreach conducted through Internet websites.

17 (c) VOLUNTARY CYBERSECURITY SELF-ASSESS-
18 MENTS.—The Director shall provide, through the Hollings
19 Manufacturing Extension Partnership, assistance to help
20 small manufacturers conduct voluntary self-assessments in
21 order to understand operating environments, cybersecurity
22 requirements, and existing vulnerabilities.

23 (d) TRANSFER OF RESEARCH FINDINGS AND EXPER-
24 TISE.—

1 (1) IN GENERAL.—The Director shall provide
2 for the transfer of technology and techniques devel-
3 oped at the National Institute of Standards and
4 Technology to Centers, and through such Centers, to
5 small manufacturers throughout the United States
6 to implement security measures that are adequate to
7 protect covered defense information, including con-
8 trolled unclassified information.

9 (2) USE OF OTHER FEDERAL EXPERTISE AND
10 CAPABILITIES.—The Director shall use, when appro-
11 priate, the expertise and capabilities that exist in
12 Federal agencies other than the Institute, and feder-
13 ally sponsored laboratories.

14 (3) AGREEMENTS.—In carrying out this sub-
15 section, the Centers may enter into agreements with
16 private industry, institutes of higher education, or a
17 State, United States territory, local, or tribal gov-
18 ernment to ensure breadth and depth of coverage to
19 the United States defense industrial base and to le-
20 verage resources.

21 (e) DEFENSE ACQUISITION WORKFORCE CYBER
22 TRAINING PROGRAM.—The Secretary of Defense, in con-
23 sultation with the Director, shall establish a cyber coun-
24 seling certification program, or approve a similar existing
25 program, to certify small business professionals and other

- 1 relevant acquisition staff within the Department of De-
- 2 fense to provide cyber planning assistance to small manu-
- 3 facturers in the defense industrial supply chain.

○