I

115TH CONGRESS
2D SESSION

H. R. 5517

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 HOUSE OF REPRESENTATIVES

APRIL 13, 2018

Mr. PANETTA (for himself and Mr. GALLAGHER) introduced the following bill; which was referred to the Committee on Science, Space, and Technology, and in addition to the Committee on Armed Services, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

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.

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 ''Enhance Cybersecurity for Small Manufacturers Act of 2018''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) According to the Bureau of Labor Statistics, there are more than 347,000 manufacturing establishments in the United States, of which 72 percent have fewer than 20 employees and 99 percent have fewer than 500 employees.

(2) Independent studies from the National Defense Industry Association, the Defense Science Board, the Alliance for Manufacturing Foresight, and the McKinsey Global Institute have highlighted—

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

(B) the vulnerability of such manufacturers to the defense industrial base for national security; and

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

(3) As of December 31, 2017, Department of Defense suppliers must comply with new, tougher cybersecurity requirements to ensure adequate security to protect controlled unclassified information relevant to defense manufacturing supply chains. The requirements call for defense suppliers to imple-

ment and create a plan of action to respond to the guidance developed by the National Institute of Standards and Technology.

(4) The Department of Commerce has found significant cybersecurity vulnerability of small manufacturers. A survey of 9,000 contract facilities documented that 6,650 small facilities lagged behind medium and large firms across a broad range of 20 cybersecurity indicators. For several indicators, fewer than half of small firms had cybersecurity measures in place.

(5) Over the past 5 years the national network of centers operating as part of the Hollings Manufacturing Extension Partnership has worked closely with the Department of Defense to bolster the resilience of the defense industrial base supply chain. Since 2013, such centers have completed more than 2,500 projects with 1,650 companies that are suppliers to the Department of Defense.

(6) In 2017, the Hollings Manufacturing Extension Partnership interacted with more than 1,000 small manufacturers on the cybersecurity requirements of the Department of Defense. This work by the Hollings Manufacturing Extension Partnership has revealed a significant lack of awareness of the

Department of Defense cybersecurity requirements and a deficiency of financial and technical resources required to manage cybersecurity risks. If cybersecurity vulnerabilities remain unaddressed, defense supply chains face a higher likelihood of serious and exploitable vulnerabilities, as well as a substantial reduction in the number of suppliers compliant with Department of Defense requirements, and thereby ineligible to provide products and services to the Department of Defense.

(7) The Hollings Manufacturing Extension Partnership is well positioned to aid suppliers of the Department of Defense in complying with cybersecurity requirements of the Department to ensure adequate security to protect controlled unclassified information relevant to defense manufacturing supply chains.

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

(a) DEFINITIONS.—In this section:

(1) CENTER.—The term ''Center'' has the meaning given such term in section 25(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278k(a)).

(2) DIRECTOR.—The term ''Director'' means the Director of the National Institute of Standards and Technology.

(3) RESOURCES.—The term ''resources'' means guidelines, tools, best practices, standards, methodologies, and other ways of providing information.

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

(5) SMALL MANUFACTURER.—The term ''small manufacturer'' means a small business concern that is a manufacturer.

(6) STATE.—The term ''State'' means each of the several States, Territories, and possessions of the United States, the District of Columbia, and the Commonwealth of Puerto Rico.

(b) DISSEMINATION OF CYBERSECURITY RESOURCES.—

(1) IN GENERAL.—The Director of the National Institute of Standards and Technology, in partnership with the Secretary of Defense and acting through the Hollings Manufacturing Extension Partnership, shall take such actions as may be necessary to address a widespread lack of awareness of cyber-

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

(2) NATIONAL REACH.—The Director shall ensure that efforts to increase awareness under paragraph (1) are carried out in each State, by disseminating clear and concise resources to help reduce cybersecurity risks faced by small manufacturers described in paragraph (1).

(3) SECTOR FOCUS.—The Director shall carry out this subsection with a focus on such industry sectors as the Director considers critical, in consultation with the Secretary of Defense.

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

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

(d) TRANSFER OF RESEARCH FINDINGS AND EXPERTISE.—

(1) IN GENERAL.—The Director shall provide for the transfer of technology and techniques developed at the National Institute of Standards and Technology to Centers, and through such Centers, to small manufacturers throughout the United States to implement security measures that are adequate to protect covered defense information, including controlled unclassified information.

(2) USE OF OTHER FEDERAL EXPERTISE AND CAPABILITIES.—The Director shall use, when appropriate, the expertise and capabilities that exist in Federal agencies other than the Institute, and federally sponsored laboratories.

(3) AGREEMENTS.—In carrying out this subsection, the Centers may enter into agreements with private industry, institutes of higher education, or a State, United States territory, local, or tribal government to ensure breadth and depth of coverage to the United States defense industrial base and to leverage resources.

(e) DEFENSE ACQUISITION WORKFORCE CYBER TRAINING PROGRAM.—The Secretary of Defense, in consultation with the Director, shall establish a cyber counseling certification program, or approve a similar existing program, to certify small business professionals and other

relevant acquisition staff within the Department of Defense to provide cyber planning assistance to small manufacturers in the defense industrial supply chain.

○