116TH CONGRESS
1ST SESSION

S. 1798

To improve cyber governance structures in the Department of Defense and to require designation of principal advisors on military cyber force matters, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 12, 2019

Mr. ROUNDS (for himself and Ms. DUCKWORTH) introduced the following bill; which was read twice and referred to the Committee on Armed Services

---

A BILL

To improve cyber governance structures in the Department of Defense and to require designation of principal advisors on military cyber force matters, 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 ''Department of Defense Principal Cyber Advisors Act of 2019''.

SEC. 2. CYBER GOVERNANCE STRUCTURES AND PRINCIPAL ADVISORS ON MILITARY CYBER FORCE MATTERS.

(a) DESIGNATION.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, each Secretary of a military department shall designate a Principal Cyber Advisor to act as the principal advisor to the Secretary of the military department on the cyber forces, cyber programs, and cybersecurity matters of the military department, including matters relating to weapons systems, enabling infrastructure, and the defense industrial base.

(2) NATURE OF POSITION.—Each Principal Cyber Advisor position under paragraph (1) shall be a senior civilian leadership position.

(b) RESPONSIBILITIES PRINCIPAL CYBER ADVISORS.—Each Principal Cyber Advisor of a military department shall be responsible for advising the Secretary of the military department and coordinating and overseeing the implementation of policy, strategies, sustainment, and plans on the following:

(1) The resourcing and training of the military cyber forces of the military department and ensuring that such resourcing and training meets the needs of United States Cyber Command.

(2) Acquisition of offensive and defensive cyber capabilities for the military cyber forces of the military department.

(3) Cybersecurity management and operations of the military department.

(4) Acquisition of cybersecurity tools and capabilities for the cybersecurity service providers of the military department.

(5) Improving and enforcing a culture of cybersecurity warfighting and responsibility throughout the military department.

(c) ADMINISTRATIVE MATTERS.—

(1) DESIGNATION OF INDIVIDUALS.—In designating a Principal Cyber Adviser under subsection (a), the Secretary of a military department may designate an individual in an existing position in the military department.

(2) COORDINATION.—The Principal Cyber Advisor of a military department shall work in close coordination with the Principal Cyber Advisor of the Department of Defense, the Chief Information Officer of the Department, relevant military service chief information officers, and other relevant military service officers to ensure service compliance with the Department of Defense Cyber Strategy.

(d) RESPONSIBILITY TO THE SENIOR ACQUISITION EXECUTIVES.—In addition to the responsibilities set forth in subsection (b), the Principal Cyber Advisor of a military department shall be responsible for advising the senior acquisition executive of the military department and, as determined by the Secretary of the military department, for advising and coordinating and overseeing the implementation of policy, strategies, sustainment, and plans for—

(1) cybersecurity of the industrial base; and

(2) cybersecurity of Department of Defense information systems and information technology services, including how cybersecurity threat information is incorporated and the development of cyber practices, cyber testing, and mitigation of cybersecurity risks.

(e) REVIEW OF CURRENT RESPONSIBILITIES.—

(1) IN GENERAL.—Not later than January 1, 2021, each Secretary of a military department shall review the military department's current governance model for cybersecurity with respect to current authorities and responsibilities.

(2) ELEMENTS.—Each review under paragraph (1) shall include the following:

(A) An assessment of whether additional changes beyond the designation of a Principal

Cyber Advisor pursuant to subsection (a) are required.

(B) Consideration of whether the current governance structure and assignment of authorities—

(i) enable effective top-down governance;

(ii) enable effective Chief Information Officer and Chief Information Security Officer action;

(iii) are adequately consolidated so that the authority and responsibility for cybersecurity risk management is clear and at an appropriate level of seniority;

(iv) provides authority to a single individual to certify compliance of Department information systems and information technology services with all current cybersecurity standards; and

(v) support efficient coordination across the military departments and services, the Office of the Secretary of Defense, the Defense Information Systems Agency, and United States Cyber Command.

(f) BRIEFING.—Not later than February 1, 2021, each Secretary of a military department shall brief the congressional defense committees on the findings of the Secretary with respect to the review conducted by the Secretary under subsection (e).

(g) DEFINITION OF CONGRESSIONAL DEFENSE COMMITTEES.—In this section, the term ''congressional defense committees'' has the meaning given such term in section 101(a) of title 10, United States Code.

○