

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.

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 “Department of Defense
5 Principal Cyber Advisors Act of 2019”.

1 **SEC. 2. CYBER GOVERNANCE STRUCTURES AND PRINCIPAL**
2 **ADVISORS ON MILITARY CYBER FORCE MAT-**
3 **TERS.**

4 (a) DESIGNATION.—

5 (1) IN GENERAL.—Not later than one year
6 after the date of the enactment of this Act, each
7 Secretary of a military department shall designate a
8 Principal Cyber Advisor to act as the principal advi-
9 sor to the Secretary of the military department on
10 the cyber forces, cyber programs, and cybersecurity
11 matters of the military department, including mat-
12 ters relating to weapons systems, enabling infra-
13 structure, and the defense industrial base.

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

17 (b) RESPONSIBILITIES PRINCIPAL CYBER ADVI-
18 SORS.—Each Principal Cyber Advisor of a military depart-
19 ment shall be responsible for advising the Secretary of the
20 military department and coordinating and overseeing the
21 implementation of policy, strategies, sustainment, and
22 plans on the following:

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

1 (2) Acquisition of offensive and defensive cyber
2 capabilities for the military cyber forces of the mili-
3 tary department.

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

6 (4) Acquisition of cybersecurity tools and capa-
7 bilities for the cybersecurity service providers of the
8 military department.

9 (5) Improving and enforcing a culture of cyber-
10 security warfighting and responsibility throughout
11 the military department.

12 (c) ADMINISTRATIVE MATTERS.—

13 (1) DESIGNATION OF INDIVIDUALS.—In desig-
14 nating a Principal Cyber Adviser under subsection
15 (a), the Secretary of a military department may des-
16 ignate an individual in an existing position in the
17 military department.

18 (2) COORDINATION.—The Principal Cyber Ad-
19 visor of a military department shall work in close co-
20 ordination with the Principal Cyber Advisor of the
21 Department of Defense, the Chief Information Offi-
22 cer of the Department, relevant military service chief
23 information officers, and other relevant military
24 service officers to ensure service compliance with the
25 Department of Defense Cyber Strategy.

1 (d) RESPONSIBILITY TO THE SENIOR ACQUISITION
2 EXECUTIVES.—In addition to the responsibilities set forth
3 in subsection (b), the Principal Cyber Advisor of a military
4 department shall be responsible for advising the senior ac-
5 quisition executive of the military department and, as de-
6 termined by the Secretary of the military department, for
7 advising and coordinating and overseeing the implementa-
8 tion of policy, strategies, sustainment, and plans for—

9 (1) cybersecurity of the industrial base; and

10 (2) cybersecurity of Department of Defense in-
11 formation systems and information technology serv-
12 ices, including how cybersecurity threat information
13 is incorporated and the development of cyber prac-
14 tices, cyber testing, and mitigation of cybersecurity
15 risks.

16 (e) REVIEW OF CURRENT RESPONSIBILITIES.—

17 (1) IN GENERAL.—Not later than January 1,
18 2021, each Secretary of a military department shall
19 review the military department’s current governance
20 model for cybersecurity with respect to current au-
21 thorities and responsibilities.

22 (2) ELEMENTS.—Each review under paragraph

23 (1) shall include the following:

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

1 Cyber Advisor pursuant to subsection (a) are
2 required.

3 (B) Consideration of whether the current
4 governance structure and assignment of au-
5 thorities—

6 (i) enable effective top-down govern-
7 ance;

8 (ii) enable effective Chief Information
9 Officer and Chief Information Security Of-
10 ficer action;

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

15 (iv) provides authority to a single in-
16 dividual to certify compliance of Depart-
17 ment information systems and information
18 technology services with all current cyber-
19 security standards; and

20 (v) support efficient coordination
21 across the military departments and serv-
22 ices, the Office of the Secretary of De-
23 fense, the Defense Information Systems
24 Agency, and United States Cyber Com-
25 mand.

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

6 (g) DEFINITION OF CONGRESSIONAL DEFENSE COM-
7 MITTEES.—In this section, the term “congressional de-
8 fense committees” has the meaning given such term in
9 section 101(a) of title 10, United States Code.

○