

119TH CONGRESS
2D SESSION

S. _____

To require the Under Secretary of Defense for Policy and the Chairman of the Joint Chiefs of Staff to submit a strategy for cyber cooperation in the Indo-Pacific region, and for other purposes.

IN THE SENATE OF THE UNITED STATES

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

A BILL

To require the Under Secretary of Defense for Policy and the Chairman of the Joint Chiefs of Staff to submit a strategy for cyber cooperation in the Indo-Pacific region, 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. STRATEGY FOR CYBER COOPERATION IN THE**
4 **INDO-PACIFIC REGION.**

5 (a) IN GENERAL.—Not later than 180 days after the
6 date of the enactment of this Act, the Under Secretary
7 of Defense for Policy and the Chairman of the Joint
8 Chiefs of Staff, in coordination with the Commander of

1 the United States Indo-Pacific Command and the Com-
2 mander of the United States Cyber Command, shall de-
3 velop, submit to the congressional defense committees (as
4 defined in section 101 of title 10, United States Code),
5 and commence implementation of a strategy to enhance
6 and institutionalize cyber cooperation between the Depart-
7 ment of Defense and allies and partners in the Indo-Pa-
8 cific region.

9 (b) ELEMENTS.—The strategy required by subsection
10 (a) shall include the following:

11 (1) An identification of the current and pro-
12 jected cyber cooperation requirements of the Depart-
13 ment of Defense in the Indo-Pacific region through
14 2040, including requirements identified in theater
15 security cooperation plans, relating to—

16 (A) defensive cyberspace operations;

17 (B) offensive cyber operations;

18 (C) secure information sharing;

19 (D) cyber training, exercises, and work-
20 force development;

21 (E) protection of critical infrastructure,
22 communications networks, and defense indus-
23 trial base networks;

24 (F) joint planning and operational integra-
25 tion; and

1 (G) command and control structures for
2 joint cyber integration.

3 (2) An identification of existing cyber coopera-
4 tion activities, agreements, and capability gaps be-
5 tween the Department of Defense and allies and
6 partners in the Indo-Pacific region.

7 (3) A strategic review of the cybersecurity ca-
8 pacity and cyber resilience of allies and partners in
9 the Indo-Pacific region that includes the following:

10 (A) With respect to each such ally or part-
11 ner—

12 (i) an assessment of the extent to
13 which the ally or partner has expressed in-
14 terest or has participated in existing
15 United States Government or Department
16 of Defense programs to assist in the the
17 expansion of cybersecurity capacity across
18 policies, technical architecture, and prac-
19 tices of the ally or partner, the results of
20 any such participation, and an identifica-
21 tion of any barriers to effective participa-
22 tion;

23 (ii) an assessment of the extent to
24 which the responsibility for cybersecurity
25 capabilities and any exposure resulting

1 from gaps in such capabilities lie with the
2 military, another government entity, or the
3 commercial sector of the ally or partner,
4 and an assessment of the manner in which
5 the structure contributes to opportunities
6 for, or risks to, collaboration with the
7 United States Armed Forces;

8 (iii) an identification of the cybersecu-
9 rity standards used by each ally or part-
10 ner, and an assessment of the extent to
11 which such standards overlap with United
12 States cybersecurity standards; and

13 (iv) in the case of an ally or partner
14 that does not have shared cybersecurity
15 standards with the United States, a review
16 of the differences between standards, the
17 manner in which such differences may cre-
18 ate barriers to interoperability and collabo-
19 ration with the Department of Defense, ex-
20 isting Department of Defense mitigation
21 measures to ensure collaboration, and rec-
22 ommendations for more permanent solu-
23 tions.

24 (B) An identification of additional re-
25 sources or authorities required to help address

1 gaps in the cybersecurity architecture or prac-
2 tices of such allies and partners, including with
3 respect to the National Guard's State Partner-
4 ship Program and consultations provided by the
5 Department of State and the Department of
6 Homeland Security.

7 (C) An identification of any capability gaps
8 of such allies and partners with respect to cy-
9 bersecurity capacity and cyber resilience that
10 the Department of Defense may be able to ad-
11 dress through security cooperation initiatives.

12 (4) An identification of—

13 (A) actions necessary to strengthen cyber
14 cooperation, interoperability, intelligence and in-
15 formation sharing, cyber defense and cybersecu-
16 rity integration, and combined cyber planning
17 with such allies and partners;

18 (B) any authorities, force posture adjust-
19 ments, organizational changes, or legislative ac-
20 tions required to improve cybersecurity in the
21 Indo-Pacific region; and

22 (C) opportunities—

23 (i) to expand bilateral and multilateral
24 cyber exercises, cyber workforce exchanges,
25 cyber capacity-building initiatives, and

1 operational collaboration with such allies
2 and partners;

3 (ii) to leverage existing security co-
4 operation mechanisms and multilateral
5 partnerships to support the objectives of
6 the strategy; and

7 (iii) to enhance collaboration between
8 the Joint Staff, the Office of the Secretary
9 of Defense, the United States Cyber Com-
10 mand, and the United States Indo-Pacific
11 Command on cybersecurity cooperation
12 with allies and partners in the Indo-Pacific
13 region.

14 (c) FUNDING PLAN.—Not later than 180 days after
15 the date of the enactment of this Act, the Under Secretary
16 of Defense for Policy and the Chairman of the Joint
17 Chiefs of Staff, in coordination with the Commander of
18 the United States Indo-Pacific Command and the Com-
19 mander of the United States Cyber Command, shall sub-
20 mit to the congressional defense committees a report that
21 includes—

22 (1) a plan for funding and resourcing the im-
23 plementation of the strategy developed under sub-
24 section (a) across the period covered by the most re-
25 cent future-years defense program submitted to Con-

1 gress under section 221 of title 10, United States
2 Code, as of the date of the report; and

3 (2) an identification of any resource gaps that
4 would impede implementation of such strategy.

5 (d) BRIEFING.—Not later than 180 days after the
6 date of the enactment of this Act, the Under Secretary
7 of Defense for Policy and the Chairman of the Joint
8 Chiefs of Staff shall provide the congressional defense
9 committees with a briefing on the strategy required by
10 subsection (a).

11 (e) IMPLEMENTATION REPORT.—Not later than
12 March 15, 2028, the Under Secretary of Defense for Pol-
13 icy and the Chairman of the Joint Chiefs of Staff shall
14 submit to the congressional defense committees a report
15 on the progress of the implementation of such strategy,
16 including—

17 (1) a description of actions taken to implement
18 the strategy;

19 (2) an assessment of remaining operational and
20 capability gaps;

21 (3) an identification of any barriers to imple-
22 mentation; and

23 (4) recommendations for any additional au-
24 thorities or resources required to carry out the strat-
25 egy.

1 (f) FORM.—The strategy, briefing, and report re-
2 quired by this section shall be submitted in unclassified
3 form but may include a classified annex.