

116TH CONGRESS
2D SESSION

S. 4226

To require the Secretary of Homeland Security to conduct an assessment of the feasibility and advisability of establishing a fund for the response to, and recovery from, a cyber state of distress, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 20, 2020

Mr. PETERS introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To require the Secretary of Homeland Security to conduct an assessment of the feasibility and advisability of establishing a fund for the response to, and recovery from, a cyber state of distress, 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 “Assessing a Cyber
5 State of Distress Act of 2020”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1 (1) APPROPRIATE CONGRESSIONAL COMMIT-
2 TEES.—The term “appropriate congressional com-
3 mittees” means—

4 (A) the Committee on Homeland Security
5 and Governmental Affairs of the Senate; and

6 (B) the Committee on Homeland Security
7 and the Committee on Oversight and Reform of
8 the House of Representatives.

9 (2) CRITICAL INFRASTRUCTURE.—The term
10 “critical infrastructure” has the meaning given the
11 term in section 1016(e) of the USA PATRIOT Act
12 (42 U.S.C. 5195c(e)).

13 (3) CYBER RESPONSE AND RECOVERY FUND.—
14 The term “Cyber Response and Recovery Fund”
15 means a fund intended to support the response and
16 recovery from a significant cyber incident, the dis-
17 bursement of which may be triggered by a declara-
18 tion of a cyber state of distress.

19 (4) CYBER STATE OF DISTRESS.—The term
20 “cyber state of distress” means a state of distress
21 that—

22 (A) begins with a Federal declaration; and

23 (B) triggers additional financial and mate-
24 rial assistance in responding to significant cyber
25 incidents.

1 (5) STATE.—The term “State” means any
2 State of the United States, the District of Columbia,
3 the Commonwealth of Puerto Rico, the Northern
4 Mariana Islands, the United States Virgin Islands,
5 Guam, American Samoa, and any other territory or
6 possession of the United States.

7 **SEC. 3. ASSESSMENT OF CYBER STATE OF DISTRESS.**

8 (a) IN GENERAL.—Not later than 180 days after the
9 enactment of this Act, the Secretary of Homeland Secu-
10 rity, in consultation with the head of any agency or non-
11 Federal entity determined appropriate by the Secretary,
12 shall conduct an assessment of the feasibility and advis-
13 ability of establishing an authority for the declaration of
14 a cyber state of distress.

15 (b) ELEMENTS.—The assessment required under
16 subsection (a) shall include—

17 (1) a review of recommendations developed by
18 the Cyberspace Solarium Commission under section
19 1652(k) of the John S. McCain National Defense
20 Authorization Act for Fiscal Year 2019 (Public Law
21 115–232; 132 Stat. 2146); and

22 (2) the development of additional recommenda-
23 tions relating to—

24 (A) the determinations that the Secretary
25 should make and any other actions that should

1 be taken before the Secretary is authorized to
2 declare or renew a cyber state of distress, in-
3 cluding whether the declaration or any renewal
4 should require congressional oversight or ap-
5 proval;

6 (B) the definition of the term “significant
7 cyber incident”, which shall include a consider-
8 ation of the threat and scope or magnitude of
9 the impact of such an incident;

10 (C) the authority for the coordination, in-
11 cluding the extent and type of coordination, of
12 the response of—

13 (i) Federal, State, local, and Tribal
14 governments, including the National
15 Guard; and

16 (ii) private entities;

17 (D) the appropriate duration of a cyber
18 state of distress and any renewal of a cyber
19 state of distress;

20 (E) whether there should be a limitation
21 on the number of renewals of a cyber state of
22 distress, with or without congressional oversight
23 or approval;

24 (F) the interaction, duplication, coordina-
25 tion, and deconfliction of—

1 (i) authorities or functions for the
2 preparation for, response to, or recovery
3 from a significant cyber incident that the
4 Secretary of Homeland Security rec-
5 ommends granting or assigning under this
6 paragraph; and

7 (ii) existing authorities or functions
8 established by law or policy that may re-
9 late to preparing for, responding to, or re-
10 covery from a significant cyber incident,
11 including under—

12 (I) the Robert T. Stafford Dis-
13 aster Relief and Emergency Assist-
14 ance Act (42 U.S.C. 5121 et seq.);

15 (II) the National Emergencies
16 Act (50 U.S.C. 1601 et seq.);

17 (III) continuity of government
18 plans;

19 (IV) other national disaster
20 plans; and

21 (V) any other Federal authority
22 the Secretary of Homeland Security
23 determines appropriate;

1 (G) appropriate exemptions from applica-
2 ble legal requirements necessary to facilitate ac-
3 tivities during a cyber state of distress;

4 (H) the scope of any allowable activities—
5 (i) in preparation for a declaration of
6 a cyber state of distress;

7 (ii) during a cyber state of distress; or

8 (iii) immediately following the termi-
9 nation of the cyber state of distress;

10 (I) the scope of any other interaction be-
11 tween Federal entities and between Federal and
12 non-Federal entities; and

13 (J) any other aspects of a cyber state of
14 distress that the Secretary of Homeland Secu-
15 rity determines relevant.

16 **SEC. 4. ASSESSMENT OF CYBER RESPONSE AND RECOVERY**
17 **FUND.**

18 (a) **IN GENERAL.**—Not later than 180 days after the
19 date of enactment of this Act, the Secretary of Homeland
20 Security shall conduct an assessment of the feasibility and
21 advisability of establishing a Cyber Response and Recov-
22 ery Fund.

23 (b) **ELEMENTS.**—The assessment required under
24 subsection (a) shall include—

1 (1) a review of recommendations developed by
2 the Cyberspace Solarium Commission under section
3 1652(k) of the John S. McCain National Defense
4 Authorization Act for Fiscal Year 2019 (Public Law
5 115–232; 132 Stat. 2146); and

6 (2) the development of additional recommenda-
7 tions relating to—

8 (A) the administration of a Cyber Re-
9 sponse and Recovery Fund;

10 (B) the eligibility of entities that may re-
11 ceive direct or indirect support under a Cyber
12 Response and Recovery Fund, including eligi-
13 bility for the receipt of direct or indirect sup-
14 port by—

15 (i) Federal entities;

16 (ii) State, local, and Tribal govern-
17 ments;

18 (iii) owners and operators of critical
19 infrastructure; and

20 (iv) private sector entities that are not
21 owners or operators of critical infrastruc-
22 ture;

23 (C) allowable expenses for a Cyber Re-
24 sponse and Recovery Fund;

1 (D) whether any entity receiving funds
2 from the Cyber Response and Recovery Fund
3 should be required to match funds or reimburse
4 any funds to the Cyber Response and Recovery
5 Fund; and

6 (E) with respect to funding available for
7 the response to, and recovery from a significant
8 cyber incident, the interaction, duplication, co-
9 ordination, and deconfliction of that funding, or
10 applications for that funding, provided—

11 (i) from a Cyber Response and Recov-
12 ery Fund; or

13 (ii) under—

14 (I) the Robert T. Stafford Dis-
15 aster Relief and Emergency Assist-
16 ance Act (42 U.S.C. 5121 et seq.);

17 (II) the National Emergencies
18 Act (50 U.S.C. 1601 et seq.); or

19 (III) any other Federal grant
20 program relating to cybersecurity or
21 natural disaster response or recovery.

22 **SEC. 5. BRIEFING.**

23 (a) IN GENERAL.—Not later than 180 days after the
24 date of enactment of this Act, the Secretary of Homeland
25 Security shall provide a briefing to each appropriate con-

1 gressional committee on the assessments carried out by
2 the Secretary of Homeland Security under sections 3 and
3 4 that includes—

4 (1) the findings from the assessments; and

5 (2) legislative proposals for the establishment
6 of—

7 (A) an authority for the declaration of a
8 cyber state of distress; and

9 (B) a Cyber Response and Recovery Fund.

10 (b) **FORMAT.**—Each briefing required under sub-
11 section (a)—

12 (1) shall be completed in a manner that is un-
13 classified; and

14 (2) may include a classified component.

○