II

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.

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 ''Assessing a Cyber State of Distress Act of 2020''.

SEC. 2. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

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

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

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

(3) CYBER RESPONSE AND RECOVERY FUND.—The term ''Cyber Response and Recovery Fund'' means a fund intended to support the response and recovery from a significant cyber incident, the disbursement of which may be triggered by a declaration of a cyber state of distress.

(4) CYBER STATE OF DISTRESS.—The term ''cyber state of distress'' means a state of distress that—

(A) begins with a Federal declaration; and

(B) triggers additional financial and material assistance in responding to significant cyber incidents.

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

SEC. 3. ASSESSMENT OF CYBER STATE OF DISTRESS.

(a) IN GENERAL.—Not later than 180 days after the enactment of this Act, the Secretary of Homeland Security, in consultation with the head of any agency or non-Federal entity determined appropriate by the Secretary, shall conduct an assessment of the feasibility and advisability of establishing an authority for the declaration of a cyber state of distress.

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

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

(2) the development of additional recommendations relating to—

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

be taken before the Secretary is authorized to declare or renew a cyber state of distress, including whether the declaration or any renewal should require congressional oversight or approval;

(B) the definition of the term ''significant cyber incident'', which shall include a consideration of the threat and scope or magnitude of the impact of such an incident;

(C) the authority for the coordination, including the extent and type of coordination, of the response of—

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

(ii) private entities;

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

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

(F) the interaction, duplication, coordination, and deconfliction of—

(i) authorities or functions for the preparation for, response to, or recovery from a significant cyber incident that the Secretary of Homeland Security recommends granting or assigning under this paragraph; and

(ii) existing authorities or functions established by law or policy that may relate to preparing for, responding to, or recovery from a significant cyber incident, including under—

(I) the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.);

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

(III) continuity of government plans;

(IV) other national disaster plans; and

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

(G) appropriate exemptions from applicable legal requirements necessary to facilitate activities during a cyber state of distress;

(H) the scope of any allowable activities—

(i) in preparation for a declaration of a cyber state of distress;

(ii) during a cyber state of distress; or

(iii) immediately following the termination of the cyber state of distress;

(I) the scope of any other interaction between Federal entities and between Federal and non-Federal entities; and

(J) any other aspects of a cyber state of distress that the Secretary of Homeland Security determines relevant.

SEC. 4. ASSESSMENT OF CYBER RESPONSE AND RECOVERY FUND.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security shall conduct an assessment of the feasibility and advisability of establishing a Cyber Response and Recovery Fund.

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

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

(2) the development of additional recommendations relating to—

(A) the administration of a Cyber Response and Recovery Fund;

(B) the eligibility of entities that may receive direct or indirect support under a Cyber Response and Recovery Fund, including eligibility for the receipt of direct or indirect support by—

(i) Federal entities;

(ii) State, local, and Tribal governments;

(iii) owners and operators of critical infrastructure; and

(iv) private sector entities that are not owners or operators of critical infrastructure;

(C) allowable expenses for a Cyber Response and Recovery Fund;

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

(E) with respect to funding available for the response to, and recovery from a significant cyber incident, the interaction, duplication, coordination, and deconfliction of that funding, or applications for that funding, provided—

(i) from a Cyber Response and Recovery Fund; or

(ii) under—

(I) the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.);

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

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

SEC. 5. BRIEFING.

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

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

(1) the findings from the assessments; and

(2) legislative proposals for the establishment of—

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

(B) a Cyber Response and Recovery Fund.

(b) FORMAT.—Each briefing required under subsection (a)—

(1) shall be completed in a manner that is unclassified; and

(2) may include a classified component.

○