117TH CONGRESS
1ST SESSION

S. 1316

To amend the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security to make a declaration of a significant incident, and for other purposes.

IN THE SENATE OF THE UNITED STATES

APRIL 22, 2021

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

---

A BILL

To amend the Homeland Security Act of 2002 to authorize the Secretary of Homeland Security to make a declaration of a significant incident, 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 ''Cyber Response and Recovery Act of 2021''.

SEC. 2. DECLARATION OF A SIGNIFICANT INCIDENT.

(a) IN GENERAL.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following:

"Subtitle C—Declaration of a Significant Incident

"SEC. 2231. DEFINITIONS.

''For the purposes of this subtitle:

''(1) ASSET RESPONSE ACTIVITY.—The term 'asset response activity' means an activity to support an entity impacted by an incident with the response to, remediation of, or recovery from, the incident, including—

''(A) furnishing technical and advisory assistance to the entity to protect the assets of the entity, mitigate vulnerabilities, and reduce the related impacts;

''(B) assessing potential risks to the critical infrastructure sector or geographic region impacted by the incident, including potential cascading effects of the incident on other critical infrastructure sectors or geographic regions;

''(C) developing courses of action to mitigate the risks assessed under subparagraph (B);

''(D) facilitating information sharing and operational coordination with entities performing threat response activities; and

''(E) providing guidance on how best to use Federal resources and capabilities in a timely, effective manner to speed recovery from the incident.

''(2) DECLARATION.—The term 'declaration' means a declaration of the Secretary under section 2232(a)(1).

''(3) DIRECTOR.—The term 'Director' means the Director of the Cybersecurity and Infrastructure Security Agency.

''(4) FEDERAL AGENCY.—The term 'Federal agency' has the meaning given the term 'agency' in section 3502 of title 44, United States Code.

''(5) FUND.—The term 'Fund' means the Cyber Response and Recovery Fund established under section 2233(a).

''(6) INCIDENT.—The term 'incident' has the meaning given the term in section 3552 of title 44, United States Code.

''(7) RENEWAL.—The term 'renewal' means a renewal of a declaration under section 2232(d).

''(8) SIGNIFICANT INCIDENT.—The term 'significant incident'—

''(A) means an incident or a group of related incidents that results, or is likely to result, in demonstrable harm to—

''(i) the national security interests, foreign relations, or economy of the United States; or

''(ii) the public confidence, civil liberties, or public health and safety of the people of the United States; and

''(B) does not include an incident or a portion of a group of related incidents that occurs on—

''(i) a national security system (as defined in section 3552 of title 44, United States Code); or

''(ii) an information system described in paragraph (2) or (3) of section 3553(e) of title 44, United States Code.

''SEC. 2232. DECLARATION.

''(a) IN GENERAL.—

''(1) DECLARATION.—The Secretary, in consultation with the National Cyber Director, may make a declaration of a significant incident in accordance with this section if the Secretary determines that—

''(A) a specific significant incident—

''(i) has occurred; or

''(ii) is likely to occur imminently; and

''(B) otherwise available resources, other than the Fund, are likely insufficient to respond effectively to, or to mitigate effectively, the specific significant incident described in subparagraph (A).

''(2) PROHIBITION ON DELEGATION.—The Secretary may not delegate the authority provided to the Secretary under paragraph (1).

''(b) ASSET RESPONSE ACTIVITIES.—Upon a declaration, the Director shall coordinate—

''(1) the asset response activities of each Federal agency in response to the specific significant incident associated with the declaration; and

''(2) with appropriate entities, which may include—

''(A) public and private entities and State and local governments with respect to the asset response activities of those entities and governments; and

''(B) Federal, State, local, and Tribal law enforcement agencies with respect to investiga-

tions and threat response activities of those law enforcement agencies.

''(c) DURATION.—Subject to subsection (d), a declaration shall terminate upon the earlier of—

''(1) a determination by the Secretary that the declaration is no longer necessary; or

''(2) the expiration of the 120-day period beginning on the date on which the Secretary makes the declaration.

''(d) RENEWAL.—The Secretary, without delegation, may renew a declaration as necessary.

''(e) PUBLICATION.—Not later than 72 hours after a declaration or a renewal, the Secretary shall publish the declaration or renewal in the Federal Register.

''(f) ADVANCE ACTIONS.—The Secretary—

''(1) shall assess the resources available to respond to a potential declaration; and

''(2) may take actions before and while a declaration is in effect to arrange or procure additional resources for asset response activities or technical assistance the Secretary determines necessary, which may include entering into standby contracts with private entities for cybersecurity services or incident responders in the event of a declaration.

"SEC. 2233. CYBER RESPONSE AND RECOVERY FUND.

"(a) IN GENERAL.—There is established a Cyber Response and Recovery Fund, which shall be available for—

"(1) the coordination of activities described in section 2232(b);

"(2) response and recovery support for the specific significant incident associated with a declaration to Federal, State, local, and Tribal, entities and public and private entities on a reimbursable or non-reimbursable basis, including through asset response activities and technical assistance, such as—

"(A) vulnerability assessments and mitigation;

"(B) technical incident mitigation;

"(C) malware analysis;

"(D) analytic support;

"(E) threat detection and hunting; and

"(F) network protections;

"(3) as the Director determines appropriate, grants for, or cooperative agreements with, Federal, State, local, and Tribal public and private entities to respond to, and recover from, the specific significant incident associated with a declaration, such as—

"(A) hardware or software to replace, update, improve, harden, or enhance the

functionality of existing hardware, software, or systems; and

''(B) technical contract personnel support; and

''(4) advance actions taken by the Secretary under section 2232(f)(2).

''(b) DEPOSITS.—Money shall be deposited into the Fund from—

''(1) appropriations to the Fund for activities of the Fund;

''(2) reimbursement from Federal agencies for the activities described in paragraphs (1), (2), and (4) of subsection (a); and

''(3) any other income incident to activities of the Fund.

''(c) SUPPLEMENT NOT SUPPLANT.—Amounts in the Fund shall be used to supplement, not supplant, other Federal, State, local, or Tribal funding for activities in response to a declaration.

''SEC. 2234. NOTIFICATION AND REPORTING.

''(a) NOTIFICATION.—Upon a declaration or renewal, the Secretary shall immediately notify the National Cyber Director and appropriate congressional committees and include in the notification—

''(1) an estimation of the planned duration of the declaration;

''(2) with respect to a notification of a declaration, the reason for the declaration, including information relating to the specific significant incident or imminent specific significant incident, including—

''(A) the operational or mission impact or anticipated impact of the specific significant incident on Federal and non-Federal entities;

''(B) if known, the perpetrator of the specific significant incident; and

''(C) the scope of the Federal and non-Federal entities impacted or anticipated to be impacted by the specific significant incident;

''(3) with respect to a notification of a renewal, the reason for the renewal;

''(4) justification as to why available resources, other than the Fund, are insufficient to respond to or mitigate the specific significant incident; and

''(5) a description of the coordination activities described in section 2232(b) that the Secretary anticipates the Director to perform.

''(b) REPORT TO CONGRESS.—Not later than 180 days after the date of a declaration or renewal, the Sec-

retary shall submit to the appropriate congressional committees a report that includes—

''(1) the reason for the declaration or renewal, including information and intelligence relating to the specific significant incident that led to the declaration or renewal;

''(2) the use of any funds from the Fund for the purpose of responding to the incidents or threat described in paragraph (1);

''(3) a description of the actions, initiatives, and projects undertaken by the Department and State and local governments and public and private entities in responding to and recovering from the specific significant incident described in paragraph (1);

''(4) an accounting of the specific obligations and outlays of the Fund; and

''(5) an analysis of—

''(A) the impact of the specific significant incident described in paragraph (1) on Federal and non-Federal entities;

''(B) the impact of the declaration or renewal on the response to, and recovery from, the specific significant incident described in paragraph (1); and

''(C) the impact of the funds made available from the Fund as a result of the declaration or renewal on the recovery from, and response to, the specific significant incident described in paragraph (1).

''(c) CLASSIFICATION.—Each notification made under subsection (a) and each report submitted under subsection (b)—

''(1) shall be in an unclassified form; and

''(2) may include a classified annex.

''(d) CONSOLIDATED REPORT.—The Secretary shall not be required to submit multiple reports under subsection (b) for multiple declarations or renewals if the Secretary determines that the declarations or renewals substantively relate to the same specific significant incident.

''(e) EXEMPTION.—The requirements of subchapter I of chapter 35 of title 44 (commonly known as the 'Paperwork Reduction Act') shall not apply to the voluntary collection of information by the Department during an investigation of, a response to, or an immediate post-response review of, the specific significant incident leading to a declaration or renewal.

''SEC. 2235. RULE OF CONSTRUCTION.

''Nothing in this subtitle shall be construed to impair or limit the ability of the Director to carry out the author-

ized activities of the Cybersecurity and Infrastructure Security Agency.

"SEC. 2236. AUTHORIZATION OF APPROPRIATIONS.

"There are authorized to be appropriated to the Fund $20,000,000 for fiscal year 2022, which shall remain available to be expended until September 30, 2028.

"SEC. 2237. SUNSET.

"The authorities granted to the Secretary or the Director under this subtitle shall expire on the date that is 7 years after the date of enactment of the Cyber Response and Recovery Act of 2021.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by adding at the end the following:

"Subtitle C—Declaration of a Significant Incident

"Sec. 2231. Definitions.
"Sec. 2232. Declaration.
"Sec. 2233. Cyber response and recovery fund.
"Sec. 2234. Notification and reporting.
"Sec. 2235. Rule of construction.
"Sec. 2236. Authorization of appropriations.
"Sec. 2237. Sunset.".

○