

117TH CONGRESS
1ST SESSION

S. _____

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

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

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.

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 “Cyber Response and
5 Recovery Act of 2021”.

6 **SEC. 2. DECLARATION OF A SIGNIFICANT INCIDENT.**

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

1 **“Subtitle C—Declaration of a**
2 **Significant Incident**

3 **“SEC. 2231. DEFINITIONS.**

4 “For the purposes of this subtitle:

5 “(1) ASSET RESPONSE ACTIVITY.—The term
6 ‘asset response activity’ means an activity to support
7 an entity impacted by an incident with the response
8 to, remediation of, or recovery from, the incident, in-
9 cluding—

10 “(A) furnishing technical and advisory as-
11 sistance to the entity to protect the assets of
12 the entity, mitigate vulnerabilities, and reduce
13 the related impacts;

14 “(B) assessing potential risks to the crit-
15 ical infrastructure sector or geographic region
16 impacted by the incident, including potential
17 cascading effects of the incident on other crit-
18 ical infrastructure sectors or geographic re-
19 gions;

20 “(C) developing courses of action to miti-
21 gate the risks assessed under subparagraph
22 (B);

23 “(D) facilitating information sharing and
24 operational coordination with entities per-
25 forming threat response activities; and

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

5 “(2) DECLARATION.—The term ‘declaration’
6 means a declaration of the Secretary under section
7 2232(a)(1).

8 “(3) DIRECTOR.—The term ‘Director’ means
9 the Director of the Cybersecurity and Infrastructure
10 Security Agency.

11 “(4) FEDERAL AGENCY.—The term ‘Federal
12 agency’ has the meaning given the term ‘agency’ in
13 section 3502 of title 44, United States Code.

14 “(5) FUND.—The term ‘Fund’ means the
15 Cyber Response and Recovery Fund established
16 under section 2233(a).

17 “(6) INCIDENT.—The term ‘incident’ has the
18 meaning given the term in section 3552 of title 44,
19 United States Code.

20 “(7) RENEWAL.—The term ‘renewal’ means a
21 renewal of a declaration under section 2232(d).

22 “(8) SIGNIFICANT INCIDENT.—The term ‘sig-
23 nificant incident’—

1 “(A) means an incident or a group of re-
2 lated incidents that results, or is likely to re-
3 sult, in demonstrable harm to—

4 “(i) the national security interests,
5 foreign relations, or economy of the United
6 States; or

7 “(ii) the public confidence, civil lib-
8 erties, or public health and safety of the
9 people of the United States; and

10 “(B) does not include an incident or a por-
11 tion of a group of related incidents that occurs
12 on—

13 “(i) a national security system (as de-
14 fined in section 3552 of title 44, United
15 States Code); or

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

19 **“SEC. 2232. DECLARATION.**

20 “(a) IN GENERAL.—

21 “(1) DECLARATION.—The Secretary, in con-
22 sultation with the National Cyber Director, may
23 make a declaration of a significant incident in ac-
24 cordance with this section if the Secretary deter-
25 mines that—

1 “(A) a specific significant incident—
2 “(i) has occurred; or
3 “(ii) is likely to occur imminently; and
4 “(B) otherwise available resources, other
5 than the Fund, are likely insufficient to respond
6 effectively to, or to mitigate effectively, the spe-
7 cific significant incident described in subpara-
8 graph (A).

9 “(2) PROHIBITION ON DELEGATION.—The Sec-
10 retary may not delegate the authority provided to
11 the Secretary under paragraph (1).

12 “(b) ASSET RESPONSE ACTIVITIES.—Upon a dec-
13 laration, the Director shall coordinate—

14 “(1) the asset response activities of each Fed-
15 eral agency in response to the specific significant in-
16 cident associated with the declaration; and

17 “(2) with appropriate entities, which may in-
18 clude—

19 “(A) public and private entities and State
20 and local governments with respect to the asset
21 response activities of those entities and govern-
22 ments; and

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

1 tions and threat response activities of those law
2 enforcement agencies.

3 “(c) DURATION.—Subject to subsection (d), a dec-
4 laration shall terminate upon the earlier of—

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

7 “(2) the expiration of the 120-day period begin-
8 ning on the date on which the Secretary makes the
9 declaration.

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

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

15 “(f) ADVANCE ACTIONS.—The Secretary—

16 “(1) shall assess the resources available to re-
17 spond to a potential declaration; and

18 “(2) may take actions before and while a dec-
19 laration is in effect to arrange or procure additional
20 resources for asset response activities or technical
21 assistance the Secretary determines necessary, which
22 may include entering into standby contracts with
23 private entities for cybersecurity services or incident
24 responders in the event of a declaration.

1 **“SEC. 2233. CYBER RESPONSE AND RECOVERY FUND.**

2 “(a) IN GENERAL.—There is established a Cyber Re-
3 sponse and Recovery Fund, which shall be available for—

4 “(1) the coordination of activities described in
5 section 2232(b);

6 “(2) response and recovery support for the spe-
7 cific significant incident associated with a declara-
8 tion to Federal, State, local, and Tribal, entities and
9 public and private entities on a reimbursable or non-
10 reimbursable basis, including through asset response
11 activities and technical assistance, such as—

12 “(A) vulnerability assessments and mitiga-
13 tion;

14 “(B) technical incident mitigation;

15 “(C) malware analysis;

16 “(D) analytic support;

17 “(E) threat detection and hunting; and

18 “(F) network protections;

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

24 “(A) hardware or software to replace, up-
25 date, improve, harden, or enhance the

1 functionality of existing hardware, software, or
2 systems; and

3 “(B) technical contract personnel support;
4 and

5 “(4) advance actions taken by the Secretary
6 under section 2232(f)(2).

7 “(b) DEPOSITS.—Money shall be deposited into the
8 Fund from—

9 “(1) appropriations to the Fund for activities of
10 the Fund;

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

14 “(3) any other income incident to activities of
15 the Fund.

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

20 **“SEC. 2234. NOTIFICATION AND REPORTING.**

21 “(a) NOTIFICATION.—Upon a declaration or renewal,
22 the Secretary shall immediately notify the National Cyber
23 Director and appropriate congressional committees and in-
24 clude in the notification—

1 “(1) an estimation of the planned duration of
2 the declaration;

3 “(2) with respect to a notification of a declara-
4 tion, the reason for the declaration, including infor-
5 mation relating to the specific significant incident or
6 imminent specific significant incident, including—

7 “(A) the operational or mission impact or
8 anticipated impact of the specific significant in-
9 cident on Federal and non-Federal entities;

10 “(B) if known, the perpetrator of the spe-
11 cific significant incident; and

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

15 “(3) with respect to a notification of a renewal,
16 the reason for the renewal;

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

20 “(5) a description of the coordination activities
21 described in section 2232(b) that the Secretary an-
22 ticipates the Director to perform.

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

1 retary shall submit to the appropriate congressional com-
2 mittees a report that includes—

3 “(1) the reason for the declaration or renewal,
4 including information and intelligence relating to the
5 specific significant incident that led to the declara-
6 tion or renewal;

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

10 “(3) a description of the actions, initiatives, and
11 projects undertaken by the Department and State
12 and local governments and public and private enti-
13 ties in responding to and recovering from the spe-
14 cific significant incident described in paragraph (1);

15 “(4) an accounting of the specific obligations
16 and outlays of the Fund; and

17 “(5) an analysis of—

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

21 “(B) the impact of the declaration or re-
22 newal on the response to, and recovery from,
23 the specific significant incident described in
24 paragraph (1); and

1 “(C) the impact of the funds made avail-
2 able from the Fund as a result of the declara-
3 tion or renewal on the recovery from, and re-
4 sponse to, the specific significant incident de-
5 scribed in paragraph (1).

6 “(c) CLASSIFICATION.—Each notification made
7 under subsection (a) and each report submitted under sub-
8 section (b)—

9 “(1) shall be in an unclassified form; and

10 “(2) may include a classified annex.

11 “(d) CONSOLIDATED REPORT.—The Secretary shall
12 not be required to submit multiple reports under sub-
13 section (b) for multiple declarations or renewals if the Sec-
14 retary determines that the declarations or renewals sub-
15 stantively relate to the same specific significant incident.

16 “(e) EXEMPTION.—The requirements of subchapter
17 I of chapter 35 of title 44 (commonly known as the ‘Pa-
18 perwork Reduction Act’) shall not apply to the voluntary
19 collection of information by the Department during an in-
20 vestigation of, a response to, or an immediate post-re-
21 >sponse review of, the specific significant incident leading
22 to a declaration or renewal.

23 “SEC. 2235. RULE OF CONSTRUCTION.

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

1 ized activities of the Cybersecurity and Infrastructure Se-
2 curity Agency.

3 **“SEC. 2236. AUTHORIZATION OF APPROPRIATIONS.**

4 “There are authorized to be appropriated to the Fund
5 \$20,000,000 for fiscal year 2022, which shall remain
6 available to be expended until September 30, 2028.

7 **“SEC. 2237. SUNSET.**

8 “The authorities granted to the Secretary or the Di-
9 rector under this subtitle shall expire on the date that is
10 7 years after the date of enactment of the Cyber Response
11 and Recovery Act of 2021.”.

12 (b) CLERICAL AMENDMENT.—The table of contents
13 in section 1(b) of the Homeland Security Act of 2002
14 (Public Law 107–296; 116 Stat. 2135) is amended by
15 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.”.