**Calendar No. 648**

| 117TH CONGRESS *2d Session* | SENATE | REPORT 117–257 |
|---|---|---|

# CYBER RESPONSE AND RECOVERY ACT

## R E P O R T

OF THE

## COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

## 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

DECEMBER 14, 2022.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
39–010 WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
SAM J. MULOPULOS, *Minority Deputy Staff Director*
WILLIAM H.W. MCKENNA, *Minority Chief Counsel*
LAURA W. KILBRIDE, *Chief Clerk*

**Calendar No. 648**

117TH CONGRESS, *2d Session* | SENATE | REPORT 117–257

# CYBER RESPONSE AND RECOVERY ACT

DECEMBER 14, 2022.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and Governmental Affairs, submitted the following

# R E P O R T

[To accompany S. 1316]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (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, having considered the same, reports favorably thereon with an amendment in the nature of a substitute, and recommends that the bill, as amended, do pass.

CONTENTS



## I. PURPOSE AND SUMMARY

S. 1316, the *Cyber Response and Recovery Act of 2021*, is intended to permit the Secretary of Homeland Security (Secretary) to declare a "significant cyber incident" in response to a serious cyber attack on public or private networks that risks the safety and security of Americans. This bill provides additional authorities to the Secretary and the Director of the Cybersecurity and Infrastructure Security Agency (CISA) to perform asset response activities, including providing, on a voluntary basis, advice, and technical assistance

to public and private entities to respond to, mitigate the effects of, or recover from serious cyber attacks.[1]

S. 1316 also establishes a Cyber Response and Recovery Fund (Fund) that the Department of Homeland Security (DHS) and CISA can use to provide direct support to public and private entities as they respond to and recover from significant cyber attacks and breaches.

## II. Background and Need for the Legislation

The United States faces a growing array of complex cybersecurity threats posed by various state and nonstate actors.[2] Recent months have seen ransomware attacks on critical energy infrastructure and food-processing facilities, data breaches affecting government agencies and millions of private citizens, and attacks on transit systems.[3] Although every cyber attack is different, the federal government can lead the way on preparing for and defending against cyber attacks by providing oversight, risk management, information sharing, and coordination.[4]

While DHS and CISA have previously provided advisory support to entities affected by significant cyber attacks, the Committee recognizes that America's national security apparatus needs additional authorities and resources to perform these functions and combat evolving cyber threats.[5] S. 1316 will accomplish this goal by providing authority to the Secretary to declare a significant cyber incident. Such a declaration will provide the Secretary with access to a dedicated Cyber Response and Recovery Fund, which can be used to furnish technical and advisory assistance, assess and mitigate potential risks to critical infrastructure, facilitate information sharing and operational coordination across affected private and public entities, and speed recovery. The bill also ensures effective communication and accountability by requiring the Secretary to notify the National Cyber Director and appropriate congressional committees with the details of any ongoing or imminent significant cyber incidents. Finally, the bill requires the Secretary to submit, within 180 days after an incident, reports describing the reason for the declaration, any actions taken, any funds used, and the effects of those actions.

---

[1] Asset response activities are activities in support of the response to, remediation of, or recovery from, the incident, including furnishing voluntary technical and advisory assistance to the entity, assessing potential risks to the critical infrastructure sector or geographic region impacted by the incident, and providing voluntary guidance on how best to use Federal resources and capabilities in a timely, effective manner to speed recovery from the incident.

[2] Congressional Research Service, *Cybersecurity: A Primer* (IF10559) (Dec. 15, 2020); Congressional Research Service, *Cybersecurity: Homeland Security Issues for the 116th Congress* (R45701) (Nov. 26, 2019).

[3] Senator Gary Peters: *Peters Presses Colonial Pipeline CEO on Recent Hack That Caused Gas Shortages and Price Increases for Millions of Americans* (June 8, 2021); JBS Paid $11 *Million in Ransom After Hackers Shut Down Meat Plants*, Washington Post (Jun. 9, 2021) (https://www.washingtonpost.com/technology/2021/06/09/jbs-11-million-ransom); Senator Gary Peters: *Peters Convenes Second Hearing with Top Federal Cybersecurity Officials to Discuss Recent Breaches and Attacks Against U.S. Systems* (May 11, 2021); Senate Permanent Subcommittee on Investigations, *How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach (2019); The M.T.A. Is Breached by Hackers as Cyberattacks Surge*, New York Times (Jun. 3, 2021) (https://www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html).

[4] Congressional Research Service, *Cybersecurity: A Primer* (IF10559) (Dec. 15, 2020); Congressional Research Service, *Cybersecurity: Homeland Security Issues for the 116th Congress* (R45701) (Nov. 26, 2019).

[5] Senator Gary Peters: *Peters & Portman Introduce Legislation to Create Significant Cyber Incident Declaration for Major Cyber-Attacks* (Apr. 23, 2021).

## III. LEGISLATIVE HISTORY

Senators Peters (D–MI) and Portman (R–OH) introduced S. 1316 on April 22, 2021. The bill was referred to the Senate Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 1316 at a business meeting on May 12, 2021. During the business meeting, a substitute amendment was offered by Senators Peters and Portman which incorporated a Sense of Congress regarding the purpose of the Cyber Response and Recovery Fund and incorporated several technical changes to clarify that only previously appropriated funds can be utilized by the Secretary when exercising the authorities granted in the bill. The Peters-Portman Substitute Amendment was adopted by unanimous consent with Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Paul, Lankford, Romney, Scott, and Hawley present.

The Committee ordered the bill, as amended, reported favorably by voice vote. The Senators present for the vote were: Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Portman, Johnson, Paul, Lankford, Romney, Scott, and Hawley.

## IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

*Section 1. Short title*

This section establishes that the bill may be cited as the "Cyber Response and Recovery Act of 2021."

*Section 2. Declaration of a Significant Incident*

This section establishes a new heading in the Homeland Security Act of 2002, which reads, "Subtitle C—Declaration of a Significant Incident."

*Section 2231. Sense of Congress*

This section describes the purpose of the bill and notes that it is intended to enable the Secretary to provide voluntary assistance to non-Federal entities affected by significant incidents.

*Section 2232. Definitions*

This section includes definitions of the terms "asset response activity," "declaration," "director," "federal agency," "fund," "incident," "renewal," and "significant incident."

*Section 2233. Declaration*

Subsection (a) determines the circumstances under which the Secretary may make a declaration of a significant incident. It also prohibits the Secretary from delegating the authority to declare a significant incident.

Subsection (b) lays out the activities that the Director of CISA will coordinate after a declaration, including the responses of Federal agencies, state and local governments and law enforcement agencies, and private entities.

Subsection (c) sets the maximum duration of a declaration at 120 days.

Subsection (d) allows the Secretary to renew a declaration, as necessary.

Subsection (e) requires the Secretary to publish a declaration or renewal in the Federal Register within 72 hours and prohibits such a publication from including the name of any affected individual or private company.

Subsection (f) allows the Secretary to take certain advance actions before and during a declaration to arrange or procure additional resources, including entering standby contracts with private entities for cybersecurity or incident response services. It also limits expenditures for those actions to money available in the Cyber Response and Recovery Fund or money otherwise appropriated to the Department.

*Section 2234. Cyber response and recovery fund*

Subsection (a) establishes the Fund and authorizes its use to assist various public and private entities with response and recovery from significant incidents. Subsection (a) establishes that the Fund can be used on a reimbursable or nonreimbursable basis for a variety of asset response and technical assistance activities, including advance actions taken by the Secretary. The Director may also distribute amounts to various public and private entities from the Fund as grants or cooperative agreements to replace, improve, or enhance hardware or software systems, or to hire technical contract personnel support.

Subsection (b) establishes that money will be deposited into the Fund only by appropriations, reimbursements for the activities described in subsection (a), or any other income incident to the activities of the Fund. Subsection (b) also establishes that expenditures will be made from available money in the Fund.

Subsection (c) specifically notes that the Fund is intended to supplement, *not supplant*, other federal and nonfederal governmental funding for activities in response to a declaration.

*Section 2235. Notification and reporting*

Subsection (a) requires the Secretary to notify the National Cyber Director and appropriate congressional committees immediately upon a declaration or renewal. The notification must include the estimated duration, reason for the declaration, estimated impact and scope of the incident, known perpetrators, a justification for why the fund will be needed to address the incident, and a description of coordination activities that the Secretary expects the Director of CISA to perform.

Subsection (b) requires the Secretary to submit a report within 180 days after any declaration or renewal to the appropriate congressional committees. The report must include: (1) the reason for the declaration or renewal; (2) the use of any funds from the Fund for activities in response to an incident (and any specific obligations and outlays of the Fund); (3) a description of what actions were taken by various entities including DHS in response to the significant incident; and (4) an analysis of the impact of the significant incident, the impact of the declaration or renewal, and the impact of the funds made available from the Fund.

Subsection (c) requires the notification and reports under subsections (b) and (c) to be unclassified, except for information in a classified annex or otherwise exempt from disclosure under the Freedom of Information Act.

Subsection (d) allows the Secretary to submit a single report under subsection (b) for multiple declarations or renewals if those declarations and renewals relate to the same significant incident.

Subsection (e) exempts from the provisions of the Paperwork Reduction Act any voluntary collection of information by DHS during an investigation, response, or post-response review of a significant incident.

*Section 2236. Rule of construction*

Notes that nothing in this bill will be construed to impair or limit the Director from carrying out the authorized activities of CISA.

*Section 2237. Authorization of appropriations*

Authorizes $20,000,000 to the Fund for fiscal year 2022, which will be available until September 30, 2028.

*Section 2238. Sunset*

Notes that the authorities granted by the bill will sunset seven years after enactment. This section also contains an addition to the table of contents for the Homeland Security Act to reflect the provisions of the bill.

## V. Evaluation of Regulatory Impact

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform bill (UMRA) and would impose no costs on state, local, or tribal governments.

## VI. Changes in Existing Law Made by the Bill, as Reported

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted is enclosed in brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

# HOMELAND SECURITY ACT OF 2002

* * * * * * *

**SEC. 1. SHORT TITLE; TABLE OF CONTENTS.**

(a) * * *

(b) Table of Contents.—The table of contents for this Act is as follows:

Sec. 1. * * *

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

* * * * * * *

# TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

## Subtitle C—Declaration of a Significant Incident

***SEC. 2231. SENSE OF CONGRESS.***

*It is the sense of Congress that—*

*(1) the purpose of this subtitle is to authorize the Secretary to declare that a significant incident has occurred and to establish the authorities that are provided under the declaration to respond to and recover from the significant incident; and*

*(2) the authorities established under this subtitle are intended to enable the Secretary to provide voluntary assistance to non-Federal entities impacted by a significant incident.*

***SEC. 2232. 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 2233(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 2234(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 2233(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. 2233. 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 for the purpose of enabling the activities described in this subtitle 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 investigations 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.—*

*(1) IN GENERAL.—Not later than 72 hours after a declaration or a renewal, the Secretary shall publish the declaration or renewal in the Federal Register.*

*(2) PROHIBITION.—A declaration or renewal published under paragraph (1) may not include the name of any affected individual or private company.*

*(f) ADVANCE ACTIONS.—*

*(1) IN GENERAL.—The Secretary—*

*(A) shall assess the resources available to respond to a potential declaration; and*

*(B) 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.*

*(2) EXPENDITURE OF FUNDS.—Any expenditure made for the purpose of paragraph (1)(B) shall be made from amounts—*

*(A) available in the Fund; or*

*(B) otherwise appropriated to the Department.*

***SEC. 2234. 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 2233(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 2233(f)(1)(B).*

*(b) DEPOSITS AND EXPENDITURES.—*

*(1) IN GENERAL.—Amounts shall be deposited into the Fund from—*

*(A) appropriations to the Fund for activities of the Fund;*

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

*(C) any other income incident to activities of the Fund.*

*(2) EXPENDITURES.—Any expenditure from the Fund shall be made from amounts that are available in the Fund from a deposit described in paragraph (1).*

*(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. 2235. 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 2233(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 Secretary 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 incident 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 with appropriate markings to indicate information that is exempt from disclosure under section 552 of title 5, United States Code (commonly known as the 'Freedom of Information Act'); 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. 2236. RULE OF CONSTRUCTION.***

*Nothing in this subtitle shall be construed to impair or limit the ability of the Director to carry out the authorized activities of the Cybersecurity and Infrastructure Security Agency.*

***SEC. 2237. 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. 2238. 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.*

* * * * * * *

○