

seq.) of title XXII of Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2150, which is classified generally to this part. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

#### CODIFICATION

Section was formerly classified to section 133 of this title prior to renumbering by Pub. L. 115–278.

#### AMENDMENTS

2022—Subsec. (b). Pub. L. 117–286 substituted “chapter 10 of title 5.” for “the Federal Advisory Committee Act.”

2018—Subsec. (h). Pub. L. 115–278, § 2(g)(9)(B)(ii), substituted “section 672 of this title” for “section 132 of this title”.

2012—Subsec. (c). Pub. L. 112–199 inserted at end “For purposes of this section a permissible use of independently obtained information includes the disclosure of such information under section 2302(b)(8) of title 5.”

2004—Subsec. (a)(1)(D)(ii)(II). Pub. L. 108–271 substituted “Government Accountability Office” for “General Accounting Office”.

#### Statutory Notes and Related Subsidiaries

##### EFFECTIVE DATE OF 2012 AMENDMENT

Amendment by Pub. L. 112–199 effective 30 days after Nov. 27, 2012, see section 202 of Pub. L. 112–199, set out as a note under section 1204 of Title 5, Government Organization and Employees.

#### § 674. No private right of action

Nothing in this part may be construed to create a private right of action for enforcement of any provision of this chapter.

(Pub. L. 107–296, title XXII, § 2225, formerly title II, § 215, Nov. 25, 2002, 116 Stat. 2155; renumbered title XXII, § 2225, Pub. L. 115–278, § 2(g)(2)(H), Nov. 16, 2018, 132 Stat. 4178.)

#### Editorial Notes

##### REFERENCES IN TEXT

This chapter, referred to in text, was in the original “this Act”, meaning Pub. L. 107–296, Nov. 25, 2002, 116 Stat. 2135, known as the Homeland Security Act of 2002, which is classified principally to this chapter. For complete classification of this Act to the Code, see Short Title note set out under section 101 of this title and Tables.

#### CODIFICATION

Section was formerly classified to section 134 of this title prior to renumbering by Pub. L. 115–278.

#### PART C—DECLARATION OF A SIGNIFICANT INCIDENT

#### § 677. Sense of Congress

It is the sense of Congress that—

(1) the purpose of this part 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 part are intended to enable the Secretary to provide voluntary assistance to non-Federal entities impacted by a significant incident.

(Pub. L. 107–296, title XXII, § 2231, as added Pub. L. 117–58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1267.)

#### § 677a. Definitions

For the purposes of this part:

##### (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 677b(a)(1) of this title.

##### (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.

##### (5) Fund

The term “Fund” means the Cyber Response and Recovery Fund established under section 677c(a) of this title.

##### (6) Incident

The term “incident” has the meaning given the term in section 3552 of title 44.

##### (7) Renewal

The term “renewal” means a renewal of a declaration under section 677b(d) of this title.

##### (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); or

(ii) an information system described in paragraph (2) or (3) of section 3553(e) of title 44.

(Pub. L. 107–296, title XXII, § 2232, as added Pub. L. 117–58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1267.)

## **§ 677b. 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 part 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; and

(3) Federal, State, local, and Tribal emergency management and response 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 from the Fund for the purpose of paragraph (1)(B) shall be made from amounts available in the Fund, and amounts available in the Fund shall be in addition to any other appropriations available to the Cybersecurity and Infrastructure Security Agency for such purpose.

(Pub. L. 107–296, title XXII, § 2233, as added Pub. L. 117–58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1268.)

## **§ 677c. 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 677b(b) of this title;

(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 677b(f)(1)(B) of this title.

### **(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; and

(B) reimbursement from Federal agencies for the activities described in paragraphs (1),

(2), and (4) of subsection (a), which shall only be from amounts made available in advance in appropriations Acts for such reimbursement.

**(2) Expenditures**

Any expenditure from the Fund for the purposes of this part shall be made from amounts available in the Fund from a deposit described in paragraph (1), and amounts available in the Fund shall be in addition to any other appropriations available to the Cybersecurity and Infrastructure Security Agency for such purposes.

**(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.

**(d) Reporting**

The Secretary shall require an entity that receives amounts from the Fund to submit a report to the Secretary that details the specific use of the amounts.

(Pub. L. 107–296, title XXII, § 2234, as added Pub. L. 117–58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1270.)

**§ 677d. 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 677b(b) of this title 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 relat-

ing 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 (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.

(Pub. L. 107–296, title XXII, § 2235, as added Pub. L. 117–58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1270.)

**§ 677e. Rule of construction**

Nothing in this part 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.

(Pub. L. 107–296, title XXII, § 2236, as added Pub. L. 117–58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1272.)

**§ 677f. Authorization of appropriations**

There are authorized to be appropriated to the Fund \$20,000,000 for fiscal year 2022 and each fis-

cal year thereafter until September 30, 2028, which shall remain available until September 30, 2028.

(Pub. L. 107-296, title XXII, § 2237, as added Pub. L. 117-58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1272.)

#### § 677g. Sunset

The authorities granted to the Secretary or the Director under this part shall expire on the date that is 7 years after November 15, 2021.

(Pub. L. 107-296, title XXII, § 2238, as added Pub. L. 117-58, div. G, title VI, § 70602(a), Nov. 15, 2021, 135 Stat. 1272.)

### PART D—CYBER INCIDENT REPORTING

#### § 681. Definitions

In this part:

##### (1) Center

The term “Center” means the center established under section 659 of this title.

##### (2) Council

The term “Council” means the Cyber Incident Reporting Council described in section 681f of this title.

##### (3) Covered cyber incident

The term “covered cyber incident” means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 681b(b) of this title.

##### (4) Covered entity

The term “covered entity” means an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21, that satisfies the definition established by the Director in the final rule issued pursuant to section 681b(b) of this title.

##### (5) Cyber incident

The term “cyber incident”—

(A) has the meaning given the term “incident” in section 659<sup>1</sup> of this title; and

(B) does not include an occurrence that imminently, but not actually, jeopardizes—

- (i) information on information systems; or
- (ii) information systems.

##### (6) Cyber threat

The term “cyber threat” has the meaning given the term “cybersecurity threat” in section 650 of this title.

##### (7) Federal entity

The term “Federal entity” has the meaning given the term in section 1501 of this title.

##### (8) Ransom payment

The term “ransom payment” means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

##### (9) Significant cyber incident

The term “significant cyber incident” means a cyber incident, or a group of related cyber incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

##### (10) Virtual currency

The term “virtual currency” means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.

##### (11) Virtual currency address

The term “virtual currency address” means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.

(Pub. L. 107-296, title XXII, § 2240, as added Pub. L. 117-103, div. Y, § 103(a)(2), Mar. 15, 2022, 136 Stat. 1039; amended Pub. L. 117-263, div. G, title LXXI, § 7143(b)(2)(N), Dec. 23, 2022, 136 Stat. 3661.)

#### Editorial Notes

##### REFERENCES IN TEXT

Section 659 of this title, referred to in par. (5)(A), was subsequently amended, and section 659(a) no longer defines the term “incident”. Reference to term, “incident”, as defined in this chapter deemed to be a reference to that term as defined in section 650(12) of this title, see section 7143(f)(2) of Pub. L. 117-263, set out as a Rule of Construction note under section 650 of this title.

##### AMENDMENTS

2022—Par. (2). Pub. L. 117-263, § 7143(b)(2)(N)(i), (ii), redesignated par. (3) as (2) and struck out former par. (2). Prior to amendment, text of par. (2) read as follows: “The term ‘cloud service provider’ means an entity offering products or services related to cloud computing, as defined by the National Institute of Standards and Technology in NIST Special Publication 800-145 and any amendatory or superseding document relating thereto.”

Pars. (3) to (5). Pub. L. 117-263, § 7143(b)(2)(N)(ii), redesignated pars. (4) to (6) as pars. (3) to (5), respectively. Former par. (3) redesignated (2).

Par. (6). Pub. L. 117-263, § 7143(b)(2)(N)(ii), (iii), redesignated par. (7) as (6) and substituted “section 650 of this title” for “section 651 of this title”. Former par. (6) redesignated (5).

Par. (7). Pub. L. 117-263, § 7143(b)(2)(N)(iv), added par. (7). Former par. (7) redesignated (6).

Par. (8). Pub. L. 117-263, § 7143(b)(2)(N)(iv), (vi), redesignated par. (13) as (8) and struck out former par. (8). Prior to amendment, text of par. (8) read as follows: “The terms ‘cyber threat indicator’, ‘cybersecurity purpose’, ‘defensive measure’, ‘Federal entity’, and ‘security vulnerability’ have the meanings given those terms in section 1501 of this title.”

Par. (9). Pub. L. 117-263, § 7143(b)(2)(N)(v), (vi), redesignated par. (16) as (9) and struck out former par. (9). Prior to amendment, text of par. (9) read as follows: “The terms ‘incident’ and ‘sharing’ have the meanings given those terms in section 659 of this title.”

Par. (10). Pub. L. 117-263, § 7143(b)(2)(N)(v), (vi), redesignated par. (18) as (10) and struck out former par. (10). Prior to amendment, text of par. (10) read as follows: “The term ‘Information Sharing and Analysis Organization’ has the meaning given the term in section 671 of this title.”

Par. (11). Pub. L. 117-263, § 7143(b)(2)(N)(v), (vi), redesignated par. (19) as (11) and struck out former par. (11).

<sup>1</sup> See References in Text note below.