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[1] 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 (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).

[1] See References in Text note below.

Prior to amendment, text of par. (11) read as follows: ''The term 'information system'—

''(A) has the meaning given the term in section 3502 of title 44; and

''(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.''

Par. (12). Pub. L. 117–263, § 7143(b)(2)(N)(v), struck out par. (12). Text read as follows: ''The term 'managed service provider' means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity (such as hosting), or in a third party data center.''

Par. (13). Pub. L. 117–263, § 7143(b)(2)(N)(vi), redesignated par. (13) as (8).

Par. (14). Pub. L. 117–263, § 7143(b)(2)(N)(v), struck out par. (14). Text read as follows: ''The term 'ransomware attack'—

''(A) means an incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

''(B) does not include any such event where the demand for payment is—

''(i) not genuine; or

''(ii) made in good faith by an entity in response to a specific request by the owner or operator of the information system.''

Par. (15). Pub. L. 117–263, § 7143(b)(2)(N)(v), struck out par. (15). Text read as follows: ''The term 'Sector Risk Management Agency' has the meaning given the term in section 651 of this title.''

Par. (16). Pub. L. 117–263, § 7143(b)(2)(N)(vi), redesignated par. (16) as (9).

Par. (17). Pub. L. 117–263, § 7143(b)(2)(N)(v), struck out par. (17). Text read as follows: ''The term 'supply chain compromise' means an incident within the supply chain of an information system that an adversary can leverage or does leverage to jeopardize the confidentiality, integrity, or availability of the information system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.''

Pars. (18), (19). Pub. L. 117–263, § 7143(b)(2)(N)(vi), redesignated pars. (18) and (19) as (10) and (11), respectively.

§ 681a. Cyber incident review

(a) Activities

The Center shall—

(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and other cybersecurity purposes, including to assess potential impact of cyber incidents on public health and safety and to enhance situational awareness of cyber threats across critical infrastructure sectors;

(2) coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments, including those utilizing virtual currencies;

(3) leverage information gathered about cyber incidents to—

(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, critical infrastructure owners and operators, cybersecurity and cyber incident response firms, and security researchers; and

(B) provide appropriate entities, including sector coordinating councils, Information Sharing and Analysis Organizations, State, local, Tribal, and territorial governments, technology providers, cybersecurity and cyber incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures, pursuant to section 681e of this title;

(4) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information, and how the Agency can most effectively support private sector cybersecurity;

(5) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar cyber incidents in the future;

(6) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

(7) with respect to covered cyber incident reports under section[1] 681b(a) and 681c of this title involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

(8) publish quarterly unclassified, public reports that describe aggregated, anonymized observations, findings, and recommendations based on covered cyber incident reports, which may be based on the unclassified information contained in the briefings required under subsection (c);

(9) proactively identify opportunities, consistent with the protections in section 681e of

[1] So in original. Probably should be ''sections''.