Homeland Security Act of 2002 which comprises this chapter.

## SUBCHAPTER XVIII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

### § 650. Definitions

Except as otherwise specifically provided, in this subchapter:

**(1) Agency**

The term ''Agency'' means the Cybersecurity and Infrastructure Security Agency.

**(2) Appropriate congressional committees**

The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Homeland Security of the House of Representatives.

**(3) Cloud service provider**

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.

**(4) Critical infrastructure information**

The term ''critical infrastructure information'' means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

**(5) Cyber threat indicator**

The term ''cyber threat indicator'' means information that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(H) any combination thereof.

**(6) Cybersecurity purpose**

The term ''cybersecurity purpose'' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

**(7) Cybersecurity risk**

The term ''cybersecurity risk''—

(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

**(8) Cybersecurity threat**

**(A) In general**

Except as provided in subparagraph (B), the term ''cybersecurity threat'' means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

**(B) Exclusion**

The term ''cybersecurity threat'' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

**(9) Defensive measure**

**(A) In general**

Except as provided in subparagraph (B), the term ''defensive measure'' means an action, device, procedure, signature, technique, or other measure applied to an infor-

mation system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

**(B) Exclusion**

The term ''defensive measure'' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

(i) the private entity, as defined in section 1501 of this title, operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

**(10) Director**

The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

**(11) Homeland Security Enterprise**

The term ''Homeland Security Enterprise'' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and Tribal government officials, private sector representatives, academics, and other policy experts.

**(12) Incident**

The term ''incident'' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

**(13) Information Sharing and Analysis Organization**

The term ''Information Sharing and Analysis Organization'' means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of an interference, a compromise, or an incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

**(14) Information system**

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.

**(15) Intelligence community**

The term ''intelligence community'' has the meaning given the term in section 3003(4) of title 50.

**(16) Malicious cyber command and control**

The term ''malicious cyber command and control'' means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

**(17) Malicious reconnaissance**

The term ''malicious reconnaissance''[1] a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

**(18) Managed service provider**

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.

**(19) Monitor**

The term ''monitor'' means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

**(20) National cybersecurity asset response activities**

The term ''national cybersecurity asset response activities'' means—

(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

(D) facilitating information sharing and operational coordination with threat response; and

(E) providing guidance on how best to utilize Federal resources and capabilities in a

[1] So in original. Probably should be followed by ''means''.

timely, effective manner to speed recovery from cybersecurity risks.

**(21) National security system**

The term ''national security system'' has the meaning given the term in section 11103 of title 40.

**(22) Ransomware attack**

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 in which 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.

**(23) Sector Risk Management Agency**

The term ''Sector Risk Management Agency'' means a Federal department or agency, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

**(24) Security control**

The term ''security control'' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

**(25) Security vulnerability**

The term ''security vulnerability'' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

**(26) Sharing**

The term ''sharing'' (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).

**(27) SLTT entity**

The term ''SLTT entity'' means a domestic government entity that is a State government, local government, Tribal government, territorial government, or any subdivision thereof.

**(28) Supply chain compromise**

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.

(Pub. L. 107–296, title XXII, § 2200, as added Pub. L. 117–263, div. G, title LXXI, § 7143(b)(1), Dec. 23, 2022, 136 Stat. 3654.)

**Statutory Notes and Related Subsidiaries**

RULE OF CONSTRUCTION

Pub. L. 117–263, div. G, title LXXI, § 7143(f), Dec. 23, 2022, 136 Stat. 3664, provided that:

''(1) INTERPRETATION OF TECHNICAL CORRECTIONS.—Nothing in the amendments made by subsections (a) through (d) [enacting this section and amending sections 195f, 321*l*, 464, 571, 624, 651 to 652a, 655, 656, 659 to 663, 665, 665b, 665d, 665g, 665i, 671, 681, 1501, 1521, and 1524 of this title, sections 278g–3a and 648 of Title 15, Commerce and Trade, section 824s–1 of Title 16, Conservation, sections 300hh–10 and 18723 of Title 42, The Public Health and Welfare, section 70101 of Title 46, Shipping, and sections 3049a and 3371a of Title 50, War and National Defense] shall be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in section 3502 of title 44, United States Code) or officer or employee of the United States on or before the date of enactment of this Act [Dec. 23, 2022].

''(2) INTERPRETATION OF REFERENCES TO DEFINITIONS.—Any reference to a term defined in the Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) on the day before the date of enactment of this Act that is defined in section 2200 of that Act [6 U.S.C. 650] pursuant to the amendments made under this Act [Pub. L. 117–263, see Tables for classification] shall be deemed to be a reference to that term as defined in section 2200 of the Homeland Security Act of 2002, as added by this Act.''

## PART A—CYBERSECURITY AND INFRASTRUCTURE SECURITY

### § 651. Definition

In this part, the term ''Cybersecurity Advisory Committee'' means the advisory committee established under section 665e(a) of this title.

(Pub. L. 107–296, title XXII, § 2201, as added Pub. L. 115–278, § 2(a), Nov. 16, 2018, 132 Stat. 4168; amended Pub. L. 116–283, div. H, title XC, § 9002(c)(2)(C), Jan. 1, 2021, 134 Stat. 4772; Pub. L. 117–150, § 2(1), June 21, 2022, 136 Stat. 1295; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(2)(B), Dec. 23, 2022, 136 Stat. 3659.)

**Editorial Notes**

AMENDMENTS

2022—Pub. L. 117–263 amended section generally. Prior to amendment, section defined critical infrastructure information, cybersecurity risk, cybersecurity threat, national cybersecurity asset response activities, Sector Risk Management Agency, sharing, and SLTT entity.

Par. (7). Pub. L. 117–150 added par. (7).

2021—Par. (5). Pub. L. 116–283 substituted ''Sector Risk Management Agency'' for ''Sector-Specific Agency'' in heading and ''Sector Risk Management Agency'' for ''Sector-Specific Agency'' in text.

**Statutory Notes and Related Subsidiaries**

RULE OF CONSTRUCTION

Nothing in amendment made by Pub. L. 117–263 to be construed to alter the authorities, responsibilities, functions, or activities of any agency (as such term is defined in 44 U.S.C. 3502) or officer or employee of the United States on or before Dec. 23, 2022, and references to terms defined in the Homeland Security Act of 2002