

other authority for reimbursable or non-reimbursable details. A nonreimbursable detail made pursuant to such paragraph shall not be considered an augmentation of the appropriations of the receiving element of the Office of the National Cyber Director.

(f) Rules of construction

Nothing in this section may be construed as—

(1) modifying any authority or responsibility, including any operational authority or responsibility of any head of a Federal department or agency;

(2) authorizing the Director or any person acting under the authority of the Director to interfere with or to direct a criminal or national security investigation, arrest, search, seizure, or disruption operation;

(3) amending a legal restriction that was in effect on the day before January 1, 2021 that requires a law enforcement agency to keep confidential information learned in the course of a criminal or national security investigation;

(4) authorizing the Director or any person acting under the authority of the Director to interfere with or to direct a military operation;

(5) authorizing the Director or any person acting under the authority of the Director to interfere with or to direct any diplomatic or consular activity;

(6) authorizing the Director or any person acting under the authority of the Director to interfere with or to direct an intelligence activity, resource, or operation; or

(7) authorizing the Director or any person acting under the authority of the Director to modify the classification of intelligence information.

(g) Definitions

In this section:

(1) The term “cybersecurity posture” means the ability to identify, to protect against, to detect, to respond to, and to recover from an intrusion in an information system the compromise of which could constitute a cyber attack or cyber campaign of significant consequence.

(2) The term “cyber attack and cyber campaign of significant consequence” means an incident or series of incidents that has the purpose or effect of—

(A) causing a significant disruption to the confidentiality, integrity, or availability of a Federal information system;

(B) harming, or otherwise significantly compromising the provision of service by, a computer or network of computers that support one or more entities in a critical infrastructure sector;

(C) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;

(D) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or

(E) otherwise constituting a significant threat to the national security, foreign pol-

icy, or economic health or financial stability of the United States.

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

(4) The term “incident response” means a government or private sector activity that detects, mitigates, or recovers from a cyber attack or cyber campaign of significant consequence.

(5) The term “information security” has the meaning given such term in section 3552 of title 44.

(6) The term “intelligence” has the meaning given such term in section 3003 of title 50.

(Pub. L. 116–283, div. A, title XVII, §1752, Jan. 1, 2021, 134 Stat. 4144; Pub. L. 117–81, div. A, title XV, §1552, Dec. 27, 2021, 135 Stat. 2070.)

Editorial Notes

CODIFICATION

Section was enacted as part of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, and not as part of the Cybersecurity Information Sharing Act of 2015 which comprises this subchapter and not as part of the Cybersecurity Act of 2015 which comprises this chapter.

Section is comprised of section 1752 of Pub. L. 116–283. Subsec. (d) of section 1752 of Pub. L. 116–283 amended section 3021 of Title 50, War and National Defense.

AMENDMENTS

2021—Subsec. (e)(1). Pub. L. 117–81, §1552(3), added subpar. (C) and redesignated former subpars. (C) to (H) as (D) to (I), respectively.

Pub. L. 117–81, §1552(1), (2), designated existing provisions as par. (1), inserted heading, redesignated former pars. (1) to (8) as subpars. (A) to (H), respectively, of par. (1), and realigned margins.

Subsec. (e)(2). Pub. L. 117–81, §1552(4), added par. (2).

§ 1501. Definitions

In this subchapter:

(1) Agency

The term “agency” has the meaning given the term in section 3502 of title 44.

(2) Antitrust laws

The term “antitrust laws”—

(A) has the meaning given the term in section 12 of title 15;

(B) includes section 45 of title 15 to the extent that section 45 of title 15 applies to unfair methods of competition; and

(C) includes any State antitrust law, but only to the extent that such law is consistent with the law referred to in subparagraph (A) or the law referred to in subparagraph (B).

(3) Appropriate Federal entities

The term “appropriate Federal entities” means the following:

(A) The Department of Commerce.

(B) The Department of Defense.

(C) The Department of Energy.

(D) The Department of Homeland Security.

(E) The Department of Justice.

(F) The Department of the Treasury.

(G) The Office of the Director of National Intelligence.

(4) 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.

(5) 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.

(6) 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.

(7) 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 information 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 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.

(8) Federal entity

The term “Federal entity” means a department or agency of the United States or any component of such department or agency.

(9) 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.

(10) Local government

The term “local government” means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

(11) 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.

(12) Malicious reconnaissance

The term “malicious reconnaissance” means 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.

(13) 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.

(14) Non-Federal entity**(A) In general**

Except as otherwise provided in this paragraph, the term “non-Federal entity” means any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof).

(B) Inclusions

The term “non-Federal entity” includes a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, American Samoa, the Northern

Mariana Islands, and any other territory or possession of the United States.

(C) Exclusion

The term “non-Federal entity” does not include a foreign power as defined in section 1801 of title 50.

(15) Private entity

(A) In general

Except as otherwise provided in this paragraph, the term “private entity” means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or non-profit entity, including an officer, employee, or agent thereof.

(B) Inclusion

The term “private entity” includes a State, tribal, or local government performing utility services, such as electric, natural gas, or water services.

(C) Exclusion

The term “private entity” does not include a foreign power as defined in section 1801 of title 50.

(16) 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.

(17) 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.

(18) Tribal

The term “tribal” has the meaning given the term “Indian tribe” in section 5304 of title 25.

(Pub. L. 114–113, div. N, title I, §102, Dec. 18, 2015, 129 Stat. 2936.)

Statutory Notes and Related Subsidiaries

SHORT TITLE

Pub. L. 114–113, div. N, §1(a), Dec. 18, 2015, 129 Stat. 2935, provided that: “This division [enacting this chapter and sections 149 and 151 of this title, amending sections 131, 148, 149, and 150 of this title, section 1029 of Title 18, Crimes and Criminal Procedure, and sections 3553 and 3554 of Title 44, Public Printing and Documents, enacting provisions set out as notes under this section and sections 101, 131, and 151 of this title and section 301 of Title 5, Government Organization and Employees] may be cited as the ‘Cybersecurity Act of 2015’.”

Pub. L. 114–113, div. N, title I, §101, Dec. 18, 2015, 129 Stat. 2936, provided that: “This title [enacting this subchapter] may be cited as the ‘Cybersecurity Information Sharing Act of 2015’.”

Pub. L. 114–113, div. N, title II, §221, Dec. 18, 2015, 129 Stat. 2963, provided that: “This subtitle [subtitle B (§§221–229) of title II of div. N of Pub. L. 114–113, enacting subchapter II of this chapter and sections 149 and 151 of this title, amending sections 148, 149, and 150 of this title and sections 3553 and 3554 of Title 44, Public Printing and Documents, and enacting provisions set out as a note under section 151 of this title] may be

cited as the ‘Federal Cybersecurity Enhancement Act of 2015’.”

§ 1502. Sharing of information by the Federal Government

(a) In general

Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, shall jointly develop and issue procedures to facilitate and promote—

(1) the timely sharing of classified cyber threat indicators and defensive measures in the possession of the Federal Government with representatives of relevant Federal entities and non-Federal entities that have appropriate security clearances;

(2) the timely sharing with relevant Federal entities and non-Federal entities of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this subchapter, in the possession of the Federal Government that may be declassified and shared at an unclassified level;

(3) the timely sharing with relevant Federal entities and non-Federal entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators and defensive measures in the possession of the Federal Government;

(4) the timely sharing with Federal entities and non-Federal entities, if appropriate, of information relating to cybersecurity threats or authorized uses under this subchapter, in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats; and

(5) the periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analyses of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this subchapter, in the possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in section 632 of title 15).

(b) Development of procedures

(1) In general

The procedures developed under subsection (a) shall—

(A) ensure the Federal Government has and maintains the capability to share cyber threat indicators and defensive measures in real time consistent with the protection of classified information;

(B) incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal entities and non-Federal entities for information sharing by the Federal Government, including sector specific information sharing and analysis centers;