

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 policy, 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). Pub. L. 117–81, §1552(1), (2), (4), designated existing provisions as par. (1) and inserted heading, redesignated former pars. (1) to (8) as subpars. (A) to (H), respectively, of par. (1) and realigned margins, and added par. (2).

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

### Statutory Notes and Related Subsidiaries

#### SHORT TITLE OF 2022 AMENDMENT

Pub. L. 117–260, §1, Dec. 21, 2022, 136 Stat. 2389, provided that: “This Act [enacting section 1526 of this title and provisions set out as notes under section 1526 of this title] may be cited as the ‘Quantum Computing Cybersecurity Preparedness Act’.”

### § 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” has the meaning given the term in section 650 of this title.

#### (5) Cybersecurity threat

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

**(6) Cyber threat indicator**

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

**(7) Defensive measure**

The term “defensive measure” has the meaning given the term in section 650 of this title.

**(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” has the meaning given the term in section 650 of this title.

**(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” has the meaning given the term in section 650 of this title.

**(12) Malicious reconnaissance**

The term “malicious reconnaissance” has the meaning given the term in section 650 of this title.

**(13) Monitor**

The term “monitor” has the meaning given the term in section 650 of this title.

**(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 per-

forming 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” has the meaning given the term in section 650 of this title.

**(17) Security vulnerability**

The term “security vulnerability” has the meaning given the term in section 650 of this title.

**(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; Pub. L. 117–263, div. G, title LXXI, § 7143(b)(4), Dec. 23, 2022, 136 Stat. 3661.)

**Editorial Notes****AMENDMENTS**

2022—Pars. (4) to (7). Pub. L. 117–263, § 7143(b)(4)(A), added pars. (4) to (7) and struck out former pars. (4) to (7) which defined cybersecurity purpose, cybersecurity threat, cyber threat indicator, and defensive measure, respectively.

Par. (9). Pub. L. 117–263, § 7143(b)(4)(B), added par. (9) and struck out former par. (9) which defined information system.

Pars. (11) to (13). Pub. L. 117–263, § 7143(b)(4)(C), added pars. (11) to (13) and struck out former pars. (11) to (13) which defined malicious cyber command and control, malicious reconnaissance, and monitor, respectively.

Pars. (16), (17). Pub. L. 117–263, § 7143(b)(4)(D), added pars. (16) and (17) and struck out former pars. (16) and (17) which defined security control and security vulnerability, respectively.

**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,