Nov. 18, 1997, 111 Stat. 2049; Pub. L. 106–65, div. C, title XXXI, § 3142(h)(2), Oct. 5, 1999, 113 Stat. 934; renumbered Pub. L. 107–314, div. D, title XLV, § 4506, and amended Pub. L. 108–136, div. C, title XXXI, § 3141(h)(7), Nov. 24, 2003, 117 Stat. 1773; Pub. L. 113–66, div. C, title XXXI, § 3121(a), Dec. 26, 2013, 127 Stat. 1060; Pub. L. 114–328, div. C, title XXXI, § 3135, Dec. 23, 2016, 130 Stat. 2771; Pub. L. 115–91, div. C, title XXXI, § 3133(b), Dec. 12, 2017, 131 Stat. 1896.)

CODIFICATION

Section was formerly set out as a note under section 7274m of Title 42, The Public Health and Welfare, prior to renumbering by Pub. L. 108–136.

AMENDMENTS

2017—Subsecs. (a)(1), (3), (b)(1). Pub. L. 115–91 substituted ''of each even-numbered year'' for ''of each year''.

2016—Subsec. (b)(1)(B). Pub. L. 114–328 amended subpar. (B) generally. Prior to amendment, subpar. (B) read as follows: ''written certification that such facilities meet the security standards and requirements of the Department of Energy.''

2013—Pub. L. 113–66 amended section generally. Prior to amendment, text read as follows: ''Not later than September 1 each year, the Secretary of Energy shall submit to the congressional defense committees the report entitled 'Annual Report to the President on the Status of Safeguards and Security of Domestic Nuclear Weapons Facilities', or any successor report to such report.''

2003—Subsec. (b). Pub. L. 108–136, § 3141(h)(7)(D), which directed the amendment of subsec. (b) by inserting ''of the National Defense Authorization Act for Fiscal Year 1998 (Public Law 105–85; 111 Stat. 2048; 42 U.S.C. 7251 note)'' after ''section 3161'', could not be executed because of the repeal of subsec. (b) by Pub. L. 106–65. See 1999 Amendment note below.

1999—Pub. L. 106–65 struck out subsec. (a) designation and heading and struck out heading and text of subsec. (b). Text read as follows: ''The Secretary shall include with each report submitted under subsection (a) in fiscal years 1998 through 2000 any comments on such report by the members of the Department of Energy Security Management Board established under section 3161 that such members consider appropriate.''

§ 2658. Repealed. Pub. L. 113–66, div. C, title XXXI, § 3132(a)(1), Dec. 26, 2013, 127 Stat. 1068

Section, Pub. L. 107–314, div. D, title XLV, § 4507, formerly Pub. L. 106–65, div. C, title XXXI, § 3152, Oct. 5, 1999, 113 Stat. 940; renumbered Pub. L. 107–314, div. D, title XLV, § 4507, and amended Pub. L. 108–136, div. C, title XXXI, § 3141(h)(8), Nov. 24, 2003, 117 Stat. 1773; Pub. L. 112–239, div. C, title XXXI, § 3131(n)(1), Jan. 2, 2013, 126 Stat. 2183, related to the annual submission and contents of a report on counterintelligence and security practices at national security laboratories.

§ 2659. Repealed. Pub. L. 114–113, div. M, title VII, § 701(f), Dec. 18, 2015, 129 Stat. 2930

Section, Pub. L. 107–314, div. D, title XLV, § 4508, formerly Pub. L. 106–65, div. C, title XXXI, § 3153, Oct. 5, 1999, 113 Stat. 940; renumbered Pub. L. 107–314, div. D, title XLV, § 4508, and amended Pub. L. 108–136, div. C, title XXXI, § 3141(h)(9), Nov. 24, 2003, 117 Stat. 1774; Pub. L. 112–239, div. C, title XXXI, § 3131(*o*)(1), Jan. 2, 2013, 126 Stat. 2183, related to report on security vulnerabilities of national security laboratory computers.

§ 2660. Repealed. Pub. L. 115–91, div. C, title XXXI, § 3135(c)(1), Dec. 12, 2017, 131 Stat. 1899

Section, Pub. L. 107–314, div. D, title XLV, § 4509, as added Pub. L. 112–239, div. C, title XXXI, § 3115(a), Jan. 2, 2013, 126 Stat. 2172; amended Pub. L. 113–291, div. C, title XXXI, § 3111, Dec. 19, 2014, 128 Stat. 3884, related to design and use of prototypes of nuclear weapons for intelligence purposes.

§ 2661. Protection of certain nuclear facilities and assets from unmanned aircraft

(a) Authority

Notwithstanding any provision of title 18, the Secretary of Energy may take such actions described in subsection (b)(1) that are necessary to mitigate the threat (as defined by the Secretary of Energy, in consultation with the Secretary of Transportation) that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset.

(b) Actions described

(1) The actions described in this paragraph are the following:

(A) Detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire, oral, or electronic communication used to control the unmanned aircraft system or unmanned aircraft.

(B) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by passive or active, and direct or indirect physical, electronic, radio, and electromagnetic means.

(C) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft.

(D) Seize or exercise control of the unmanned aircraft system or unmanned aircraft.

(E) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.

(F) Use reasonable force to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.

(2) The Secretary of Energy shall develop the actions described in paragraph (1) in coordination with the Secretary of Transportation.

(c) Forfeiture

Any unmanned aircraft system or unmanned aircraft described in subsection (a) that is seized by the Secretary of Energy is subject to forfeiture to the United States.

(d) Regulations

The Secretary of Energy and the Secretary of Transportation may prescribe regulations and shall issue guidance in the respective areas of each Secretary to carry out this section.

(e) Definitions

In this section:

(1) The term ''covered facility or asset'' means any facility or asset that is—

(A) identified by the Secretary of Energy for purposes of this section;

(B) located in the United States (including the territories and possessions of the United States); and

(C) owned by the United States or contracted to the United States, to store or use special nuclear material.

(2) The terms ''unmanned aircraft'' and ''unmanned aircraft system'' have the meanings given those terms in section 331 of the FAA Modernization and Reform Act of 2012 (Public Law 112–95; 49 U.S.C. 40101[1] note).

(Pub. L. 107–314, div. D, title XLV, § 4510, as added Pub. L. 114–328, div. C, title XXXI, § 3112(a), Dec. 23, 2016, 130 Stat. 2756.)

REFERENCES IN TEXT

Section 331 of the FAA Modernization and Reform Act of 2012 (Public Law 112–95), referred to in subsec. (e)(2), which was formerly set out in a note under section 40101 of Title 49, Transportation, was transferred and is now set out in a note under section 44802 of Title 49.

§ 2662. Reporting on penetrations of networks of contractors and subcontractors

(a) Procedures for reporting penetrations

The Administrator shall establish procedures that require each contractor and subcontractor to report to the Chief Information Officer when a covered network of the contractor or subcontractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.

(b) Establishment of criteria for covered networks

(1) In general

The Administrator shall, in consultation with the officials specified in paragraph (2), establish criteria for covered networks to be subject to the procedures for reporting penetrations under subsection (a).

(2) Officials specified

The officials specified in this paragraph are the following officials of the Administration:

(A) The Deputy Administrator for Defense Programs.

(B) The Associate Administrator for Acquisition and Project Management.

(C) The Chief Information Officer.

(D) Any other official of the Administration the Administrator considers necessary.

(c) Procedure requirements

(1) Rapid reporting

(A) In general

The procedures established pursuant to subsection (a) shall require each contractor or subcontractor to submit to the Chief Information Officer a report on each successful penetration of a covered network of the contractor or subcontractor that meets the criteria established pursuant to subsection (b) not later than 60 days after the discovery of the successful penetration.

(B) Elements

Subject to subparagraph (C), each report required by subparagraph (A) with respect to a successful penetration of a covered network of a contractor or subcontractor shall include the following:

(i) A description of the technique or method used in such penetration.

(ii) A sample of the malicious software, if discovered and isolated by the contractor or subcontractor, involved in such penetration.

(iii) A summary of information created by or for the Administration in connection with any program of the Administration that has been potentially compromised as a result of such penetration.

(C) Avoidance of delays in reporting

If a contractor or subcontractor is not able to obtain all of the information required by subparagraph (B) to be included in a report required by subparagraph (A) by the date that is 60 days after the discovery of a successful penetration of a covered network of the contractor or subcontractor, the contractor or subcontractor shall—

(i) include in the report all information available as of that date; and

(ii) provide to the Chief Information Officer the additional information required by subparagraph (B) as the information becomes available.

(2) Access to equipment and information by Administration personnel

Concurrent with the establishment of the procedures pursuant to subsection (a), the Administrator shall establish procedures to be used if information owned by the Administration was in use during or at risk as a result of the successful penetration of a covered network—

(A) in order to—

(i) in the case of a penetration of a covered network of a management and operating contractor, enhance the access of personnel of the Administration to Government-owned equipment and information; and

(ii) in the case of a penetration of a covered network of a contractor or subcontractor that is not a management and operating contractor, facilitate the access of personnel of the Administration to the equipment and information of the contractor or subcontractor; and

(B) which shall—

(i) include mechanisms for personnel of the Administration to, upon request, obtain access to equipment or information of a contractor or subcontractor necessary to conduct forensic analysis in addition to any analysis conducted by the contractor or subcontractor;

(ii) provide that a contractor or subcontractor is only required to provide access to equipment or information as described in clause (i) to determine whether information created by or for the Administration in connection with any program of the Administration was successfully exfiltrated from a network of the contractor or subcontractor and, if so, what information was exfiltrated; and

[1] See References in Text note below.