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 Repealed.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 Repealed.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.)

Editorial Notes

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.

[1] See References in Text note below.

(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

(iii) provide for the reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person.

(3) Dissemination of information

The procedures established pursuant to subsection (a) shall allow for limiting the dissemination of information obtained or derived through such procedures so that such information may be disseminated only to entities—

(A) with missions that may be affected by such information;

(B) that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(C) that conduct counterintelligence or law enforcement investigations; or

(D) for national security purposes, including cyber situational awareness and defense purposes.

(d) Definitions

In this section:

(1) Chief Information Officer

The term ''Chief Information Officer'' means the Associate Administrator for Information Management and Chief Information Officer of the Administration.

(2) Contractor

The term ''contractor'' means a private entity that has entered into a contract or contractual action of any kind with the Administration to furnish supplies, equipment, materials, or services of any kind.

(3) Covered network

The term ''covered network'' includes any network or information system that accesses, receives, or stores—

(A) classified information; or

(B) sensitive unclassified information germane to any program of the Administration, as determined by the Administrator.

(4) Subcontractor

The term ''subcontractor'' means a private entity that has entered into a contract or contractual action with a contractor or another subcontractor to furnish supplies, equipment, materials, or services of any kind in connec-

tion with another contract in support of any program of the Administration.

(Pub. L. 107–314, div. D, title XLV, § 4511, as added Pub. L. 116–283, div. C, title XXXI, § 3131(a), Jan. 1, 2021, 134 Stat. 4383.)

PART B—CLASSIFIED INFORMATION

§ 2671. Review of certain documents before declassification and release

(a) In general

The Secretary of Energy shall ensure that, before a document of the Department of Energy that contains national security information is released or declassified, such document is reviewed to determine whether it contains Restricted Data.

(b) Limitation on declassification

The Secretary may not implement the automatic declassification provisions of Executive Order No. 13526 (50 U.S.C. 3161 note) if the Secretary determines that such implementation could result in the automatic declassification and release of documents containing Restricted Data.

(Pub. L. 107–314, div. D, title XLV, § 4521, formerly Pub. L. 104–106, div. C, title XXXI, § 3155, Feb. 10, 1996, 110 Stat. 625; renumbered Pub. L. 107–314, div. D, title XLV, § 4521, by Pub. L. 108–136, div. C, title XXXI, § 3141(h)(11), Nov. 24, 2003, 117 Stat. 1774; amended Pub. L. 112–239, div. C, title XXXI, § 3131(p), Jan. 2, 2013, 126 Stat. 2183; Pub. L. 113–66, div. C, title XXXI, § 3146(a)(2)(G), Dec. 26, 2013, 127 Stat. 1073; Pub. L. 113–291, div. C, title XXXI, § 3142(*l*), Dec. 19, 2014, 128 Stat. 3901.)

Editorial Notes

CODIFICATION

Section was formerly set out as a note under section 2162 of Title 42, The Public Health and Welfare, prior to renumbering by Pub. L. 108–136.

AMENDMENTS

2014—Subsec. (b). Pub. L. 113–291 substituted ''Executive Order No. 13526 (50 U.S.C. 3161 note)'' for ''Executive Order 12958''.

2013—Subsecs. (a), (b). Pub. L. 113–66 substituted ''Restricted Data'' for ''restricted data''.

Subsec. (c). Pub. L. 112–239 struck out subsec. (c), which defined ''restricted data''.

§ 2672. Protection against inadvertent release of Restricted Data and Formerly Restricted Data

(a) Plan for protection against release

The Secretary of Energy and the Archivist of the United States shall, after consultation with the members of the National Security Council and in consultation with the Secretary of Defense and the heads of other appropriate Federal agencies, develop a plan to prevent the inadvertent release of records containing Restricted Data or Formerly Restricted Data during the automatic declassification of records under Executive Order No. 13526 (50 U.S.C. 3161 note).

(b) Plan elements

The plan under subsection (a) shall include the following:

(1) The actions to be taken in order to ensure that records subject to Executive Order No. 13526 are reviewed on a page-by-page basis for Restricted Data and Formerly Restricted Data unless they have been determined to be highly unlikely to contain Restricted Data or Formerly Restricted Data.

(2) The criteria and process by which documents are determined to be highly unlikely to contain Restricted Data or Formerly Restricted Data.

(3) The actions to be taken in order to ensure proper training, supervision, and evaluation of personnel engaged in declassification under that Executive order so that such personnel recognize Restricted Data and Formerly Restricted Data.

(4) The extent to which automated declassification technologies will be used under that Executive order to protect Restricted Data and Formerly Restricted Data from inadvertent release.

(5) Procedures for periodic review and evaluation by the Secretary of Energy, in consultation with the Director of the Information Security Oversight Office of the National Archives and Records Administration, of compliance by Federal agencies with the plan.

(6) Procedures for resolving disagreements among Federal agencies regarding declassification procedures and decisions under the plan.

(7) The funding, personnel, and other resources required to carry out the plan.

(8) A timetable for implementation of the plan.

(c) Limitation on declassification of certain records

(1) Effective on October 17, 1998, and except as provided in paragraph (3), a record referred to in subsection (a) may not be declassified unless the agency having custody of the record reviews the record on a page-by-page basis to ensure that the record does not contain Restricted Data or Formerly Restricted Data.

(2) Any record determined as a result of a review under paragraph (1) to contain Restricted Data or Formerly Restricted Data may not be declassified until the Secretary of Energy, in conjunction with the head of the agency having custody of the record, determines that the document is suitable for declassification.

(3) After the date occurring 60 days after the submission of the plan required by subsection (a) to the committees referred to in paragraphs (1) and (2) of subsection (d), the requirement under paragraph (1) to review a record on a page-by-page basis shall not apply in the case of a record determined, under the actions specified in the plan pursuant to subsection (b)(1), to be a record that is highly unlikely to contain Restricted Data or Formerly Restricted Data.

(d) Submission of plan

The Secretary of Energy shall submit the plan required under subsection (a) to the following:

(1) The Committee on Armed Services of the Senate.

(2) The Committee on Armed Services of the House of Representatives.

(3) The Assistant to the President for National Security Affairs.