2018—Subsecs. (h), (i). Pub. L. 115–232, § 3113(a)(1), (2), added subsec. (h) and redesignated former subsec. (h) as (i).

Subsec. (i)(2). Pub. L. 115–232, § 3113(a)(3), struck out subpar. (A) designation and heading ''In general'', substituted ''The term'' for ''Except as provided in subparagraph (B), the term'', redesignated cls. (i) and (ii) as subpars. (A) and (B), respectively, realigned margins, and struck out former subpar. (B). Prior to amendment, text of subpar. (B) read as follows: ''The term 'major atomic energy defense acquisition program' does not include a project covered by Department of Energy Order 413.3 (or a successor order) for the acquisition of capital assets for atomic energy defense activities.''

2014—Subsec. (h)(1) to (3). Pub. L. 113–291 added par. (1) and redesignated former pars. (1) and (2) as (2) and (3), respectively.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE OF 2018 AMENDMENT

Pub. L. 115–232, div. C, title XXXI, § 3113(b), Aug. 13, 2018, 132 Stat. 2290, provided that: ''The amendments made by subsection (a) [amending this section] shall take effect on the date that is 18 months after the date of the enactment of this Act [Aug. 13, 2018].''

§ 2412. Cybersecurity Risk Inventory, Assessment, and Mitigation Working Group

(a) Establishment

There is in the Administration a working group, to be known as the ''Cybersecurity Risk Inventory, Assessment, and Mitigation Working Group'' (referred to in this section as the ''working group'').

(b) Membership

Members of the working group shall include—

(1) the Deputy Administrator for Defense Programs;

(2) the Associate Administrator for Information Management and Chief Information Officer; and

(3) such other personnel of the Administration as are determined appropriate for inclusion in the working group by the Chairperson.

(c) Chairperson

The Deputy Administrator for Defense Programs shall serve as the Chairperson of the working group, except that the Administrator may designate another member of the working group to serve as Chairperson in lieu of the Deputy Administrator if the Administrator determines it is appropriate to do so.

(d) Comprehensive strategy

The working group shall prepare a comprehensive strategy for inventorying the range of systems of the Administration that are potentially at risk in the operational technology and nuclear weapons information technology environments, assessing the systems at risk based on mission impact, and implementing risk mitigation actions. Such strategy shall incorporate key elements of effective cybersecurity risk management strategies, as identified by the Government Accountability Office, including the specification of—

(1) goals, objectives, activities, and performance measures;

(2) organizational roles, responsibilities, and coordination;

(3) resources needed to implement the strategy through 2034; and

(4) detailed milestones and schedules for completion of tasks.

(e) Submission to Congress

(1) Interim briefing

Not later than 120 days after December 22, 2023, the working group shall provide to the congressional defense committees a briefing on the plan of the working group to develop the strategy required under subsection (d).

(2) Completed strategy

Not later than April 1, 2025, the working group shall submit the congressional defense committees a copy of the completed strategy.

(f) Termination

The working group shall terminate on a date determined by the Administrator that is not earlier than the date that is five years after December 22, 2023.

(Pub. L. 106–65, div. C, title XXXII, § 3222, as added Pub. L. 118–31, div. C, title XXXI, § 3113, Dec. 22, 2023, 137 Stat. 789.)

SUBCHAPTER II—MATTERS RELATING TO SECURITY

§ 2421. Protection of national security information

(a) Policies and procedures required

The Administrator shall establish procedures to ensure the maximum protection of classified information in the possession of the Administration.

(b) Prompt reporting

The Administrator shall establish procedures to ensure prompt reporting to the Administrator of any significant problem, abuse, violation of law or Executive order, or deficiency relating to the management of classified information by personnel of the Administration.

(Pub. L. 106–65, div. C, title XXXII, § 3231, Oct. 5, 1999, 113 Stat. 960.)

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective Mar. 1, 2000, see section 3299 of Pub. L. 106–65, set out as a note under section 2401 of this title.

§ 2422. Office of Defense Nuclear Security

(a) Establishment

There is within the Administration an Office of Defense Nuclear Security, headed by a Chief appointed by the Secretary of Energy. The Administrator shall recommend to the Secretary suitable candidates for such position.

(b) Chief of Defense Nuclear Security

(1) The head of the Office of Defense Nuclear Security is the Chief of Defense Nuclear Security, who shall report to the Administrator and shall implement the security policies directed by the Secretary and Administrator.

(2) The Chief shall have direct access to the Secretary and all other officials of the Department and the contractors of the Department concerning security matters.

(3) The Chief shall be responsible for the development and implementation of security programs for the Administration, including the protection, control and accounting of materials, and for the physical security for all facilities of the Administration.

(Pub. L. 106–65, div. C, title XXXII, § 3232, Oct. 5, 1999, 113 Stat. 960; Pub. L. 109–364, div. C, title XXXI, § 3117(b)(1), Oct. 17, 2006, 120 Stat. 2507; Pub. L. 118–31, div. C, title XXXI, § 3111(2), Dec. 22, 2023, 137 Stat. 788.)

Editorial Notes

AMENDMENTS

2023—Subsec. (b)(3). Pub. L. 118–31 struck out ''and cyber'' after ''physical''.

2006—Pub. L. 109–364, § 3117(b)(1)(A), struck out ''Office of Defense Nuclear Counterintelligence and'' before ''Office of Defense Nuclear Security'' in section catchline.

Subsec. (a). Pub. L. 109–364, § 3117(b)(1)(B), added subsec. (a) and struck out heading and text of former subsec. (a). Text read as follows:

''(1) There are within the Administration—

''(A) an Office of Defense Nuclear Counterintelligence; and

''(B) an Office of Defense Nuclear Security.

''(2) Each office established under paragraph (1) shall be headed by a Chief appointed by the Secretary of Energy. The Administrator shall recommend to the Secretary suitable candidates for each such position.''

Subsecs. (b), (c). Pub. L. 109–364, § 3117(b)(1)(C), (D), redesignated subsec. (c) as (b) and struck out former subsec. (b) which related to the Chief of Defense Nuclear Counterintelligence.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective Mar. 1, 2000, see section 3299 of Pub. L. 106–65, set out as a note under section 2401 of this title.

§ 2423. Counterintelligence programs

(a) National security laboratories and nuclear weapons production facilities

The Secretary of Energy shall, at each national security laboratory and nuclear weapons production facility, establish and maintain a counterintelligence program adequate to protect national security information at that laboratory or production facility.

(b) Other facilities

The Secretary of Energy shall, at each Department facility not described in subsection (a) at which Restricted Data is located, assign an employee of the Office of Intelligence and Counterintelligence of the Department of Energy who shall be responsible for and assess counterintelligence matters at that facility.

(Pub. L. 106–65, div. C, title XXXII, § 3233, Oct. 5, 1999, 113 Stat. 961; Pub. L. 109–364, div. C, title XXXI, § 3117(a)(2)(C), (c), Oct. 17, 2006, 120 Stat. 2507, 2508; Pub. L. 111–84, div. C, title XXXI, § 3121, Oct. 28, 2009, 123 Stat. 2710; Pub. L. 116–92, div. E, title LXVII, § 6744(a), Dec. 20, 2019, 133 Stat. 2241.)

Editorial Notes

AMENDMENTS

2019—Subsec. (b). Pub. L. 116–92 substituted ''Department facility'' for ''Administration facility'' and inserted ''Intelligence and'' after ''the Office of''.

2009—Pub. L. 111–84 amended Pub. L. 109–364, § 3117(a), see 2006 Amendment note below.

2006—Pub. L. 109–364, § 3117(a), which, in par. (2), directed amendment of this section by substituting ''Administrator'' for ''Secretary of Energy'' in subsecs. (a) and (b) and ''Administration'' for ''Office of Counterintelligence of the Department of Energy'' in subsec. (b), effective Sept. 30, 2010, was amended generally by Pub. L. 111–84, and as so amended, no longer contains a par. (2) or amends this section.

Pub. L. 109–364, § 3117(c), substituted ''Secretary of Energy'' for ''Administrator'' in subsecs. (a) and (b) and ''Office of Counterintelligence of the Department of Energy'' for ''Office of Defense Nuclear Counterintelligence'' in subsec. (b).

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section effective Mar. 1, 2000, see section 3299 of Pub. L. 106–65, set out as a note under section 2401 of this title.

§ 2424. Procedures relating to access by individuals to classified areas and information of Administration

The Administrator shall establish appropriate procedures to ensure that any individual is not permitted unescorted access to any classified area, or access to classified information, of the Administration until that individual has been verified to hold the appropriate security clearances.

(Pub. L. 106–65, div. C, title XXXII, § 3234, Oct. 5, 1999, 113 Stat. 961.)

§ 2425. Government access to information on Administration computers

(a) Procedures required

The Administrator shall establish procedures to govern access to information on Administration computers. Those procedures shall, at a minimum, provide that any individual who has access to information on an Administration computer shall be required as a condition of such access to provide to the Administrator written consent which permits access by an authorized investigative agency to any Administration computer used in the performance of the duties of such employee during the period of that individual's access to information on an Administration computer and for a period of three years thereafter.

(b) Expectation of privacy in Administration computers

Notwithstanding any other provision of law (including any provision of law enacted by the Electronic Communications Privacy Act of 1986 (Public Law 99–508; 100 Stat. 1848)), no user of an Administration computer shall have any expectation of privacy in the use of that computer.

(c) Definition

For purposes of this section, the term ''authorized investigative agency'' means an agency authorized by law or regulation to conduct a counterintelligence investigation or investigations of persons who are proposed for access to classified information to ascertain whether such persons satisfy the criteria for obtaining and retaining access to such information.