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.