

Subsec. (c)(12), (13). Pub. L. 113–293, §327(2), (3), added par. (12) and redesignated former par. (12) as (13).

PERSONNEL INFORMATION NOTIFICATION POLICY BY THE  
DIRECTOR OF NATIONAL INTELLIGENCE

Pub. L. 114–113, div. M, title III, §308, Dec. 18, 2015, 129 Stat. 2917, provided that:

“(a) DIRECTIVE REQUIRED.—The Director of National Intelligence shall issue a directive containing a written policy for the timely notification to the congressional intelligence committees of the identities of individuals occupying senior level positions within the intelligence community.

“(b) SENIOR LEVEL POSITION.—In identifying positions that are senior level positions in the intelligence community for purposes of the directive required under subsection (a), the Director of National Intelligence shall consider whether a position—

“(1) constitutes the head of an entity or a significant component within an agency;

“(2) is involved in the management or oversight of matters of significant import to the leadership of an entity of the intelligence community;

“(3) provides significant responsibility on behalf of the intelligence community;

“(4) requires the management of a significant number of personnel or funds;

“(5) requires responsibility management or oversight of sensitive intelligence activities; and

“(6) is held by an individual designated as a senior intelligence management official as such term is defined in section 368(a)(6) of the Intelligence Authorization Act for Fiscal Year 2010 (Public Law 111–259; 50 U.S.C. 404i–1 [now 50 U.S.C. 3051] note).

“(c) NOTIFICATION.—The Director shall ensure that each notification under the directive issued under subsection (a) includes each of the following:

“(1) The name of the individual occupying the position.

“(2) Any previous senior level position held by the individual, if applicable, or the position held by the individual immediately prior to the appointment.

“(3) The position to be occupied by the individual.

“(4) Any other information the Director determines appropriate.

“(d) RELATIONSHIP TO OTHER LAWS.—The directive issued under subsection (a) and any amendment to such directive shall be consistent with the provisions of the National Security Act of 1947 (50 U.S.C. 401 [now 50 U.S.C. 3001] et seq.).

“(e) SUBMISSION.—Not later than 90 days after the date of the enactment of this Act [Dec. 18, 2015], the Director shall submit to the congressional intelligence committees the directive issued under subsection (a).”

[For definitions of “congressional intelligence committees” and “intelligence community” as used in section 308 of div. M of Pub. L. 114–113, set out above, see section 2 of div. M of Pub. L. 114–113, set out as a note under section 3003 of this title.]

IMPLEMENTATION

Pub. L. 111–259, title III, §305(b), Oct. 7, 2010, 124 Stat. 2661, provided that: “The first assessment required to be submitted under section 506B(b) of the National Security Act of 1947 [50 U.S.C. 3098(b)], as added by subsection (a), shall be submitted to the congressional intelligence committees at the time that the President submits to Congress the budget for fiscal year 2012 pursuant to section 1105 of title 31, United States Code.”

[For definition of “congressional intelligence committees” as used in section 305(b) of Pub. L. 111–259, set out above, see section 2 of Pub. L. 111–259, set out as a note under section 3003 of this title.]

**§ 3099. Vulnerability assessments of major systems**

**(a) Initial vulnerability assessments**

(1)(A) Except as provided in subparagraph (B), the Director of National Intelligence shall con-

duct and submit to the congressional intelligence committees an initial vulnerability assessment for each major system and its significant items of supply—

(i) except as provided in clause (ii), prior to the completion of Milestone B or an equivalent acquisition decision for the major system; or

(ii) prior to the date that is 1 year after October 7, 2010, in the case of a major system for which Milestone B or an equivalent acquisition decision—

(I) was completed prior to such date; or

(II) is completed on a date during the 180-day period following such date.

(B) The Director may submit to the congressional intelligence committees an initial vulnerability assessment required by clause (ii) of subparagraph (A) not later than 180 days after the date such assessment is required to be submitted under such clause if the Director notifies the congressional intelligence committees of the extension of the submission date under this subparagraph and provides a justification for such extension.

(C) The initial vulnerability assessment of a major system and its significant items of supply shall include use of an analysis-based approach to—

(i) identify vulnerabilities;

(ii) define exploitation potential;

(iii) examine the system’s potential effectiveness;

(iv) determine overall vulnerability; and

(v) make recommendations for risk reduction.

(2) If an initial vulnerability assessment for a major system is not submitted to the congressional intelligence committees as required by paragraph (1), funds appropriated for the acquisition of the major system may not be obligated for a major contract related to the major system. Such prohibition on the obligation of funds for the acquisition of the major system shall cease to apply on the date on which the congressional intelligence committees receive the initial vulnerability assessment.

**(b) Subsequent vulnerability assessments**

(1) The Director of National Intelligence shall, periodically throughout the procurement of a major system or if the Director determines that a change in circumstances warrants the issuance of a subsequent vulnerability assessment, conduct a subsequent vulnerability assessment of each major system and its significant items of supply within the National Intelligence Program.

(2) Upon the request of a congressional intelligence committee, the Director of National Intelligence may, if appropriate, recertify the previous vulnerability assessment or may conduct a subsequent vulnerability assessment of a particular major system and its significant items of supply within the National Intelligence Program.

(3) Any subsequent vulnerability assessment of a major system and its significant items of supply shall include use of an analysis-based approach and, if applicable, a testing-based ap-

proach, to monitor the exploitation potential of such system and reexamine the factors described in clauses (i) through (v) of subsection (a)(1)(C).

**(c) Major system management**

The Director of National Intelligence shall give due consideration to the vulnerability assessments prepared for a given major system when developing and determining the National Intelligence Program budget.

**(d) Congressional oversight**

(1) The Director of National Intelligence shall provide to the congressional intelligence committees a copy of each vulnerability assessment conducted under subsection (a) or (b) not later than 10 days after the date of the completion of such assessment.

(2) The Director of National Intelligence shall provide the congressional intelligence committees with a proposed schedule for subsequent periodic vulnerability assessments of a major system under subsection (b)(1) when providing such committees with the initial vulnerability assessment under subsection (a) of such system as required by paragraph (1).

**(e) Definitions**

In this section:

(1) The term “item of supply” has the meaning given that term in section 4(10)<sup>1</sup> of the Office of Federal Procurement Policy Act (41 U.S.C. 403(10)).

(2) The term “major contract” means each of the 6 largest prime, associate, or Government-furnished equipment contracts under a major system that is in excess of \$40,000,000 and that is not a firm, fixed price contract.

(3) The term “major system” has the meaning given that term in section 3097(e) of this title.

(4) The term “Milestone B” means a decision to enter into major system development and demonstration pursuant to guidance prescribed by the Director of National Intelligence.

(5) The term “vulnerability assessment” means the process of identifying and quantifying vulnerabilities in a major system and its significant items of supply.

(July 26, 1947, ch. 343, title V, § 506C, as added Pub. L. 111-259, title III, § 321(a)(1), Oct. 7, 2010, 124 Stat. 2667.)

REFERENCES IN TEXT

Section 4(10) of the Office of Federal Procurement Policy Act, referred to in subsec. (e)(1), which was classified to section 403(10) of former Title 41, Public Contracts, was repealed and reenacted as sections 108 and 115 of Title 41, Public Contracts, by Pub. L. 111-350, §§ 3, 7(b), Jan. 4, 2011, 124 Stat. 3677, 3855.

CODIFICATION

Section was formerly classified to section 415a-5 of this title prior to editorial reclassification and renumbering as this section.

**§ 3100. Intelligence community business system transformation**

**(a) Limitation on obligation of funds**

(1) Subject to paragraph (3), no funds appropriated to any element of the intelligence com-

munity may be obligated for an intelligence community business system transformation that will have a total cost in excess of \$3,000,000 unless—

(A) the Director of the Office of Business Transformation of the Office of the Director of National Intelligence makes a certification described in paragraph (2) with respect to such intelligence community business system transformation; and

(B) such certification is approved by the board established under subsection (f).

(2) The certification described in this paragraph for an intelligence community business system transformation is a certification made by the Director of the Office of Business Transformation of the Office of the Director of National Intelligence that the intelligence community business system transformation—

(A) complies with the enterprise architecture under subsection (b) and such other policies and standards that the Director of National Intelligence considers appropriate; or

(B) is necessary—

(i) to achieve a critical national security capability or address a critical requirement; or

(ii) to prevent a significant adverse effect on a project that is needed to achieve an essential capability, taking into consideration any alternative solutions for preventing such adverse effect.

(3) With respect to a fiscal year after fiscal year 2010, the amount referred to in paragraph (1) in the matter preceding subparagraph (A) shall be equal to the sum of—

(A) the amount in effect under such paragraph (1) for the preceding fiscal year (determined after application of this paragraph), plus

(B) such amount multiplied by the annual percentage increase in the consumer price index (all items; U.S. city average) as of September of the previous fiscal year.

**(b) Enterprise architecture for intelligence community business systems**

(1) The Director of National Intelligence shall, acting through the board established under subsection (f), develop and implement an enterprise architecture to cover all intelligence community business systems, and the functions and activities supported by such business systems. The enterprise architecture shall be sufficiently defined to effectively guide, constrain, and permit implementation of interoperable intelligence community business system solutions, consistent with applicable policies and procedures established by the Director of the Office of Management and Budget.

(2) The enterprise architecture under paragraph (1) shall include the following:

(A) An information infrastructure that will enable the intelligence community to—

(i) comply with all Federal accounting, financial management, and reporting requirements;

(ii) routinely produce timely, accurate, and reliable financial information for management purposes;

<sup>1</sup> See References in Text note below.