

Pub. L. 102-172, title VIII, §8014, Nov. 26, 1991, 105 Stat. 1174.

Pub. L. 101-511, title VIII, §8015, Nov. 5, 1990, 104 Stat. 1878.

Pub. L. 101-165, title IX, §9022, Nov. 21, 1989, 103 Stat. 1134.

Pub. L. 100-463, title VIII, §8035, Oct. 1, 1988, 102 Stat. 2270-23.

Pub. L. 100-202, §101(b) [title VIII, §8037], Dec. 22, 1987, 101 Stat. 1329-43, 1329-68.

### § 3328. Study or plan of surrender; use of appropriations

No part of the funds appropriated in any act shall be used to pay (1) any person, firm, or corporation, or any combinations of persons, firms, or corporations, to conduct a study or to plan when and how or in what circumstances the Government of the United States should surrender this country and its people to any foreign power, (2) the salary or compensation of any employee or official of the Government of the United States who proposes or contracts or who has entered into contracts for the making of studies or plans for the surrender by the Government of the United States of this country and its people to any foreign power in any event or under any circumstances.

(Pub. L. 85-766, ch. XVI, §1602, Aug. 27, 1958, 72 Stat. 884.)

#### CODIFICATION

Section was formerly classified to section 407 of this title prior to editorial reclassification and renumbering as this section.

### § 3329. Intelligence community contracting

#### (a) In general

The Director of National Intelligence shall direct that elements of the intelligence community, whenever compatible with the national security interests of the United States and consistent with the operational and security concerns related to the conduct of intelligence activities, and where fiscally sound, shall award contracts in a manner that would maximize the procurement of products in the United States.

#### (b) Intelligence community defined

In this section, the term “intelligence community” has the meaning given that term in section 3003(4) of this title.

(Pub. L. 102-183, title IV, §403, Dec. 4, 1991, 105 Stat. 1267; Pub. L. 111-259, title VIII, §810, Oct. 7, 2010, 124 Stat. 2750.)

#### CODIFICATION

Section was formerly classified to section 403-2 of this title prior to editorial reclassification and renumbering as this section.

#### PRIOR PROVISIONS

Provisions similar to those in this section were contained in the following prior authorization act: Pub. L. 102-88, title IV, §404, Aug. 14, 1991, 105 Stat. 434.

#### AMENDMENTS

2010—Pub. L. 111-259 added subsec. (b), designated existing provisions as subsec. (a), inserted heading, substituted “Director of National Intelligence” for “Director of Central Intelligence” and “intelligence community” for “Intelligence Community”, and struck out at

end “For purposes of this provision, the term ‘Intelligence Community’ has the same meaning as set forth in paragraph 3.4(f) of Executive Order 12333, dated December 4, 1981, or successor orders.”

#### ENHANCED PROCUREMENT AUTHORITY TO MANAGE SUPPLY CHAIN RISK

Pub. L. 112-87, title III, §309, Jan. 3, 2012, 125 Stat. 1883, provided that:

“(a) DEFINITIONS.—In this section:

“(1) COVERED AGENCY.—The term ‘covered agency’ means any element of the intelligence community other than an element within the Department of Defense.

“(2) COVERED ITEM OF SUPPLY.—The term ‘covered item of supply’ means an item of information technology (as that term is defined in section 11101 of title 40, United States Code) that is purchased for inclusion in a covered system, and the loss of integrity of which could result in a supply chain risk for a covered system.

“(3) COVERED PROCUREMENT.—The term ‘covered procurement’ means—

“(A) a source selection for a covered system or a covered item of supply involving either a performance specification, as provided in section 3306(a)(3)(B) of title 41, United States Code, or an evaluation factor, as provided in section 3306(b)(1) of such title, relating to supply chain risk;

“(B) the consideration of proposals for and issuance of a task or delivery order for a covered system or a covered item of supply, as provided in section 4106(d)(3) of title 41, United States Code, where the task or delivery order contract concerned includes a contract clause establishing a requirement relating to supply chain risk; or

“(C) any contract action involving a contract for a covered system or a covered item of supply where such contract includes a clause establishing requirements relating to supply chain risk.

“(4) COVERED PROCUREMENT ACTION.—The term ‘covered procurement action’ means any of the following actions, if the action takes place in the course of conducting a covered procurement:

“(A) The exclusion of a source that fails to meet qualifications standards established in accordance with the requirements of section 3311 of title 41, United States Code, for the purpose of reducing supply chain risk in the acquisition of covered systems.

“(B) The exclusion of a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk in the evaluation of proposals for the award of a contract or the issuance of a task or delivery order.

“(C) The decision to withhold consent for a contractor to subcontract with a particular source or to direct a contractor for a covered system to exclude a particular source from consideration for a subcontract under the contract.

“(5) COVERED SYSTEM.—The term ‘covered system’ means a national security system, as that term is defined in [former] section 3542(b) of title 44, United States Code [see now 44 U.S.C. 3552(b)].

“(6) SUPPLY CHAIN RISK.—The term ‘supply chain risk’ means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

“(b) AUTHORITY.—Subject to subsection (c) and in consultation with the Director of National Intelligence, the head of a covered agency may, in conducting intelligence and intelligence-related activities—

“(1) carry out a covered procurement action; and

“(2) limit, notwithstanding any other provision of law, in whole or in part, the disclosure of information

relating to the basis for carrying out a covered procurement action.

“(c) DETERMINATION AND NOTIFICATION.—The head of a covered agency may exercise the authority provided in subsection (b) only after—

“(1) any appropriate consultation with procurement or other relevant officials of the covered agency;

“(2) making a determination in writing, which may be in classified form, that—

“(A) use of the authority in subsection (b)(1) is necessary to protect national security by reducing supply chain risk;

“(B) less intrusive measures are not reasonably available to reduce such supply chain risk; and

“(C) in a case where the head of the covered agency plans to limit disclosure of information under subsection (b)(2), the risk to national security due to the disclosure of such information outweighs the risk due to not disclosing such information;

“(3) notifying the Director of National Intelligence that there is a significant supply chain risk to the covered system concerned, unless the head of the covered agency making the determination is the Director of National Intelligence; and

“(4) providing a notice, which may be in classified form, of the determination made under paragraph (2) to the congressional intelligence committees that includes a summary of the basis for the determination, including a discussion of less intrusive measures that were considered and why they were not reasonably available to reduce supply chain risk.

“(d) DELEGATION.—The head of a covered agency may not delegate the authority provided in subsection (b) or the responsibility to make a determination under subsection (c) to an official below the level of the service acquisition executive for the agency concerned.

“(e) SAVINGS.—The authority under this section is in addition to any other authority under any other provision of law. The authority under this section shall not be construed to alter or effect the exercise of any other provision of law.

“(f) EFFECTIVE DATE.—The requirements of this section shall take effect on the date that is 180 days after the date of the enactment of this Act [Jan. 3, 2012] and shall apply to contracts that are awarded on or after such date.

“(g) SUNSET.—The authority provided in this section shall expire on the date that section 806 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111-383; 10 U.S.C. 2304 note) expires.”

[For definitions of “intelligence community” and “congressional intelligence committees” as used in section 309 of Pub. L. 112-87, set out above, see section 2 of Pub. L. 112-87, set out as a note under section 3003 of this title.]

### § 3330. Reports to the intelligence community on penetrations of networks and information systems of certain contractors

#### (a) Procedures for reporting penetrations

The Director of National Intelligence shall establish procedures that require each cleared intelligence contractor to report to an element of the intelligence community designated by the Director for purposes of such procedures when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.

#### (b) Networks and information systems subject to reporting

The Director of National Intelligence shall, in consultation with appropriate officials, establish criteria for covered networks to be subject to the procedures for reporting system penetrations under subsection (a).

#### (c) Procedure requirements

##### (1) Rapid reporting

The procedures established pursuant to subsection (a) shall require each cleared intelligence contractor to rapidly report to an element of the intelligence community designated pursuant to subsection (a) of each successful penetration of the network or information systems of such contractor that meet the criteria established pursuant to subsection (b). Each such report shall include the following:

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

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

(C) A summary of information created by or for such element in connection with any program of such element that has been potentially compromised due to such penetration.

##### (2) Access to equipment and information by intelligence community personnel

The procedures established pursuant to subsection (a) shall—

(A) include mechanisms for intelligence community personnel to, upon request, obtain access to equipment or information of a cleared intelligence contractor necessary to conduct forensic analysis in addition to any analysis conducted by such contractor;

(B) provide that a cleared intelligence contractor is only required to provide access to equipment or information as described in subparagraph (A) to determine whether information created by or for an element of the intelligence community in connection with any intelligence community program was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated; and

(C) provide for the reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person (other than the name of the suspected perpetrator of the penetration).

##### (3) Limitation on dissemination of certain information

The procedures established pursuant to subsection (a) shall prohibit the dissemination outside the intelligence community of information obtained or derived through such procedures that is not created by or for the intelligence community except—

(A) with the approval of the contractor providing such information;

(B) to the congressional intelligence committees or the Subcommittees on Defense of the Committees on Appropriations of the House of Representatives and the Senate for such committees and such Subcommittees to perform oversight; or

(C) to law enforcement agencies to investigate a penetration reported under this section.