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.''

Statutory Notes and Related Subsidiaries

ENHANCED PROCUREMENT AUTHORITY TO MANAGE SUPPLY CHAIN RISK

Pub. L. 112–87, title III, § 309, Jan. 3, 2012, 125 Stat. 1883, formerly set out as a note under this section, was transferred to section 3334e 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.

(d) Issuance of procedures and establishment of criteria

(1) In general

Not later than 90 days after July 7, 2014, the Director of National Intelligence shall establish the procedures required under subsection (a) and the criteria required under subsection (b).

(2) Applicability date

The requirements of this section shall apply on the date on which the Director of National Intelligence establishes the procedures required under this section.

(e) Coordination with the Secretary of Defense to prevent duplicate reporting

Not later than 180 days after July 7, 2014, the Director of National Intelligence and the Secretary of Defense shall establish procedures to permit a contractor that is a cleared intelligence contractor and a cleared defense contractor under section 941 of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112–239; 10 U.S.C. 2224 note) to submit a single report that satisfies the requirements of this section and such section 941 for an incident of penetration of network or information system.

(f) Definitions

In this section:

(1) Cleared intelligence contractor

The term ''cleared intelligence contractor'' means a private entity granted clearance by the Director of National Intelligence or the head of an element of the intelligence community to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of an element of the intelligence community.

(2) Covered network

The term ''covered network'' means a network or information system of a cleared intelligence contractor that contains or processes information created by or for an element of the intelligence community with respect to which such contractor is required to apply enhanced protection.

(g) Savings clauses

Nothing in this section shall be construed to alter or limit any otherwise authorized access by government personnel to networks or information systems owned or operated by a contractor that processes or stores government data.

(Pub. L. 113–126, title III, § 325, July 7, 2014, 128 Stat. 1402.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of ''intelligence community'' and ''congressional intelligence committees'' as used in this section, see section 2 of Pub. L. 113–126, set out as a note under section 3003 of this title.

§ 3331. Management of intelligence community personnel

(a) Multi-sector workforce initiative

(1) Requirement

Beginning on October 1, 2018, the Director of National Intelligence shall improve management of the workforce of the intelligence community by enabling elements of the intelligence community to build and maintain an appropriate mix between employees of the United States Government and core contractors.

(2) Briefing to Congress

Not later than July 1, 2017, and each 120 days thereafter until July 1, 2018, the Director of National Intelligence shall brief the congressional intelligence committees on the initiative required by paragraph (1).

(b) Management based on workload requirements and authorized funding

(1) In general

Beginning on October 1, 2018, the personnel levels of the intelligence community shall be managed each fiscal year on the basis of—

(A) the workload required to carry out the functions and activities of the intelligence community; and

(B) the funds made available to the intelligence community in accordance with section 3094 of this title.

(2) Prohibition on constraints or limitations

Beginning on October 1, 2018, the management of such personnel in the intelligence community in any fiscal year shall not be subject to an externally imposed constraint or limitation expressed in terms of man years, end strength, full-time equivalent positions, or maximum number of employees.

(c) Briefing and report to Congress

Not later than 180 days after May 5, 2017, the Director of National Intelligence shall issue a written report and provide a briefing to the congressional intelligence committees on—

(1) the methodology used to calculate the number of civilian and contractor full-time equivalent positions in the intelligence community;

(2) the cost analysis tool used to calculate personnel costs in the intelligence community; and

(3) the plans of the Director of National Intelligence and the head of each element of the intelligence community to implement a multi-sector workforce as required by subsections (a) and (b).

(d) Report

Not later than 240 days after May 5, 2017, the Inspector General of the Intelligence Community shall submit to the congressional intelligence committees a written report on the accuracy of intelligence community data for the numbers and costs associated with the civilian and contractor workforce in each element of the intelligence community.

(Pub. L. 115–31, div. N, title III, § 306, May 5, 2017, 131 Stat. 812.)

Statutory Notes and Related Subsidiaries

DEFINITIONS

For definitions of ''intelligence community'' and ''congressional intelligence committees'' as used in this section, see section 2 of div. N of Pub. L. 115–31, set out as a note under section 3003 of this title.

§ 3332. Guidance and reporting requirement regarding the interactions between the intelligence community and entertainment industry

(a) Definitions

In this section:

(1) Engagement

The term ''engagement''—

(A) means any significant interaction between an element of the intelligence community and an entertainment industry entity for the purposes of contributing to an entertainment product intended to be heard, read, viewed, or otherwise experienced by the public; and

(B) does not include routine inquiries made by the press or news media to the public affairs office of an intelligence community.

(2) Entertainment industry entity

The term ''entertainment industry entity'' means an entity that creates, produces, pro-