fined 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.

(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.)

DEFINITIONS

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

SUBCHAPTER III—SECURITY CLEARANCES AND CLASSIFIED INFORMATION

§ 3341. Security clearances

(a) Definitions

In this section:

(1) The term ''agency'' means—

(A) an executive agency (as that term is defined in section 105 of title 5);

(B) a military department (as that term is defined in section 102 of title 5); and

(C) an element of the intelligence community.

(2) The term ''authorized investigative agency'' means an agency designated by the head of the agency selected pursuant to subsection (b) to conduct a counterintelligence investigation or investigation 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.

(3) The term ''authorized adjudicative agency'' means an agency authorized by law, regulation, or direction of the Director of National Intelligence to determine eligibility for access to classified information in accordance with Executive Order 12968.

(4) The term ''highly sensitive program'' means—

(A) a government program designated as a Special Access Program (as that term is defined in section 4.1(h) of Executive Order 12958 or any successor Executive order); or

(B) a government program that applies restrictions required for—

(i) restricted data (as that term is defined in section 2014(y) of title 42;[1] or

(ii) other information commonly referred to as ''sensitive compartmented information''.

(5) The term ''current investigation file'' means, with respect to a security clearance, a file on an investigation or adjudication that has been conducted during—

(A) the 5-year period beginning on the date the security clearance was granted, in the case of a Top Secret Clearance, or the date access was granted to a highly sensitive program;

(B) the 10-year period beginning on the date the security clearance was granted in the case of a Secret Clearance; and

(C) the 15-year period beginning on the date the security clearance was granted in the case of a Confidential Clearance.

(6) The term ''personnel security investigation'' means any investigation required for the purpose of determining the eligibility of any military, civilian, or government contractor personnel to access classified information.

[1] So in original. There probably should be a closing parenthesis before the semicolon.