''(3) Mechanisms for protection against compromise of information systems through the supply chain or cyber attack by acquiring and improving automated tools for—

''(A) assuring the security of software and software applications during software development;

''(B) detecting vulnerabilities during testing of software; and

''(C) detecting intrusions during real-time monitoring of software applications.

''(4) Mechanisms providing the Department of Defense with the capabilities—

''(A) to monitor systems and applications in order to detect and defeat attempts to penetrate or disable such systems and applications; and

''(B) to ensure that such monitoring capabilities are integrated into the Department of Defense system of cyber defense-in-depth capabilities.

''(5) An update to Committee for National Security Systems Instruction No. 4009, entitled 'National Information Assurance Glossary', to include a standard definition for software security assurance.

''(6) Either—

''(A) mechanisms to ensure that vulnerable Mission Assurance Category III information systems, if penetrated, cannot be used as a foundation for penetration of protected covered systems, and means for assessing the effectiveness of such mechanisms; or

''(B) plans to address critical vulnerabilities in Mission Assurance Category III information systems to prevent their use for intrusions of Mission Assurance Category I systems and Mission Assurance Category II systems.

''(7) A funding mechanism for remediation of critical software assurance vulnerabilities in legacy systems.

''(d) REPORT.—Not later than October 1, 2011, the Secretary of Defense shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a report on the strategy required by subsection (a). The report shall include the following:

''(1) A description of the current status of the strategy required by subsection (a) and of the implementation of the strategy, including a description of the role of the strategy in the risk management by the Department regarding the supply chain and in operational planning for cyber security.

''(2) A description of the risks, if any, that the Department will accept in the strategy due to limitations on funds or other applicable constraints.''

INSTITUTE FOR DEFENSE COMPUTER SECURITY AND INFORMATION PROTECTION

Pub. L. 106–398, § 1 [[div. A], title IX, § 921], Oct. 30, 2000, 114 Stat. 1654, 1654A–233, provided that:

''(a) ESTABLISHMENT.—The Secretary of Defense shall establish an Institute for Defense Computer Security and Information Protection.

''(b) MISSION.—The Secretary shall require the institute—

''(1) to conduct research and technology development that is relevant to foreseeable computer and network security requirements and information assurance requirements of the Department of Defense with a principal focus on areas not being carried out by other organizations in the private or public sector; and

''(2) to facilitate the exchange of information regarding cyberthreats, technology, tools, and other relevant issues.

''(c) CONTRACTOR OPERATION.—The Secretary shall enter into a contract with a not-for-profit entity, or a consortium of not-for-profit entities, to organize and operate the institute. The Secretary shall use competitive procedures for the selection of the contractor to the extent determined necessary by the Secretary.

''(d) FUNDING.—Of the amount authorized to be appropriated by section 301(5) [114 Stat. 1654A–52], $5,000,000 shall be available for the Institute for Defense Computer Security and Information Protection.

''(e) REPORT.—Not later than April 1, 2001, the Secretary shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] the Secretary's plan for implementing this section.''

§ 2224a. Information security: continued applicability of expiring Governmentwide requirements to the Department of Defense

(a) IN GENERAL.—The provisions of subchapter II[1] of chapter 35 of title 44 shall continue to apply through September 30, 2004, with respect to the Department of Defense, notwithstanding the expiration of authority under section 3536[1] of such title.

(b) RESPONSIBILITIES.—In administering the provisions of subchapter II[1] of chapter 35 of title 44 with respect to the Department of Defense after the expiration of authority under section 3536[1] of such title, the Secretary of Defense shall perform the duties set forth in that subchapter for the Director of the Office of Management and Budget.

(Added Pub. L. 107–314, div. A, title X, § 1052(b)(1), Dec. 2, 2002, 116 Stat. 2648.)

REFERENCES IN TEXT

Provisions relating to the expiration of authority of subchapter II of chapter 35 of title 44, referred to in text, did not appear in section 3536 of title 44 subsequent to the general revision of subchapter II by Pub. L. 107–296, title X, § 1001(b)(1), Nov. 25, 2002, 116 Stat. 2259. Subchapter II, as revised by Pub. L. 107–296, was repealed and a new subchapter II enacted by Pub. L. 113–283, § 2(a), Dec. 18, 2014, 128 Stat. 3073.

§ 2225. Information technology purchases: tracking and management

(a) COLLECTION OF DATA REQUIRED.—To improve tracking and management of information technology products and services by the Department of Defense, the Secretary of Defense shall provide for the collection of the data described in subsection (b) for each purchase of such products or services made by a military department or Defense Agency in excess of the simplified acquisition threshold, regardless of whether such a purchase is made in the form of a contract, task order, delivery order, military interdepartmental purchase request, or any other form of interagency agreement.

(b) DATA TO BE COLLECTED.—The data required to be collected under subsection (a) includes the following:

(1) The products or services purchased.

(2) Whether the products or services are categorized as commercially available off-the-shelf items, other commercial items, nondevelopmental items other than commercial items, other noncommercial items, or services.

(3) The total dollar amount of the purchase.

(4) The form of contracting action used to make the purchase.

(5) In the case of a purchase made through an agency other than the Department of Defense—

[1] See References in Text note below.