H.R.6523

Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Introduced in House - IH)

Print Subscribe Share/Save

H.R.6523
Latest Title: Ike Skelton National Defense Authorization Act for Fiscal Year 2011
Sponsor: Rep Skelton, Ike [MO-4] (introduced 12/15/2010)   Cosponsors (None)
Latest Major Action: 12/15/2010 Referred to House committee. Status: Referred to the Committee on Armed Services, and in addition to the Committee on the Budget, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.

Jump to: Summary, Major Actions, All Actions, Titles, Cosponsors, Committees, Related Bill Details, Amendments

---

SUMMARY:

NONE

MAJOR ACTIONS:

NONE

ALL ACTIONS:
12/15/2010:
Referred to the Committee on Armed Services, and in addition to the Committee on the Budget, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.
12/15/2010:
Referred to House Armed Services
12/15/2010:
Referred to House Budget

SEC. 932. STRATEGY ON COMPUTER SOFTWARE ASSURANCE.

(a) Strategy Required- The Secretary of Defense shall develop and implement, by not later than October 1, 2011, a strategy for assuring the security of software and software-based applications for all covered systems.

(b) Covered Systems- For purposes of this section, a covered system is any critical information system or weapon system of the Department of Defense, including the following:

(1) A major system, as that term is defined in section 2302(5) of title 10, United States Code.

(2) A national security system, as that term is defined in section 3542(b)(2) of title 44, United States Code.

(3) Any Department of Defense information system categorized as Mission Assurance Category I.

(4) Any Department of Defense information system categorized as Mission Assurance Category II in accordance with Department of Defense Directive 8500.01E.

(c) Elements- The strategy required by subsection (a) shall include the following:

(1) Policy and regulations on the following:

(A) Software assurance generally.

(B) Contract requirements for software assurance for covered systems in development and production.

(C) Inclusion of software assurance in milestone reviews and milestone approvals.

(D) Rigorous test and evaluation of software assurance in development, acceptance, and operational tests.

(E) Certification and accreditation requirements for software assurance for new systems and for updates for legacy systems, including mechanisms to monitor and enforce reciprocity of certification and accreditation processes among the military departments and Defense Agencies.

(F) Remediation in legacy systems of critical software assurance deficiencies that are defined as critical in accordance with the Application Security Technical Implementation Guide of the Defense Information Systems Agency.

(2) Allocation of adequate facilities and other resources for test and evaluation and certification and accreditation of software to meet applicable requirements for research and development, systems acquisition, and operations.

(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 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.