§ 2223. Information technology: additional responsibilities of Chief Information Officers

(a) Additional Responsibilities of Chief Information Officer of Department of Defense.— In addition to the responsibilities provided for in chapter 35 of title 44 and in section 11315 of title 40, the Chief Information Officer of the Department of Defense shall—

(1) review and provide recommendations to the Secretary of Defense on Department of Defense budget requests for information technology and national security systems;
(2) ensure the interoperability of information technology and national security systems throughout the Department of Defense;
(3) ensure that information technology and national security systems standards that will apply throughout the Department of Defense are prescribed;
(4) provide for the elimination of duplicate information technology and national security systems within and between the military departments and Defense Agencies; and
(5) maintain a consolidated inventory of Department of Defense mission critical and mission essential information systems, identify interfaces between those systems and other information systems, and develop and maintain contingency plans for responding to a disruption in the operation of any of those information systems.

(b) Additional Responsibilities of Chief Information Officer of Military Departments.— In addition to the responsibilities provided for in chapter 35 of title 44 and in section 11315 of title 40, the Chief Information Officer of a military department, with respect to the military department concerned, shall—

(1) review budget requests for all information technology and national security systems;
(2) ensure that information technology and national security systems are in compliance with standards of the Government and the Department of Defense;
(3) ensure that information technology and national security systems are interoperable with other relevant information technology and national security systems of the Government and the Department of Defense; and
(4) coordinate with the Joint Staff with respect to information technology and national security systems.

(c) Definitions.— In this section:

(1) The term “Chief Information Officer” means the senior official designated by the Secretary of Defense or a Secretary of a military department pursuant to section 3506 of title 44.
(2) The term “information technology” has the meaning given that term by section 11101 of title 40.
(3) The term “national security system” has the meaning given that term by section 3542 (b)(2) of title 44.


Amendments

2006—Subsec. (c)(3). Pub. L. 109–364 substituted “section 3542 (b)(2) of title 44” for “section 11103 of title 40”.

(10 USC 2223)


Effective Date


Ozone Widget Framework


“(a) Mechanism for Internet Publication of Information for Development of Analysis Tools and Applications.—The Chief Information Officer of the Department of Defense, acting through the Director of the Defense Information Systems Agency, shall implement a mechanism to publish and maintain on the public Internet the application programming interface specifications, a developer’s toolkit, source code, and such other information on, and resources for, the Ozone Widget Framework (OWF) as the Chief Information Officer considers necessary to permit individuals and companies to develop, integrate, and test analysis tools and applications for use by the Department of Defense and the elements of the intelligence community.

“(b) Process for Voluntary Contribution of Improvements by Private Sector.—In addition to the requirement under subsection (a), the Chief Information Officer shall also establish a process by which private individuals and companies may voluntarily contribute the following:

“(1) Improvements to the source code and documentation for the Ozone Widget Framework.

“(2) Alternative or compatible implementations of the published application programming interface specifications for the Framework.

“(c) Encouragement of Use and Development.—The Chief Information Officer shall, whenever practicable, encourage and foster the use, support, development, and enhancement of the Ozone Widget Framework by the computer industry and commercial information technology vendors, including the development of tools that are compatible with the Framework.”

Continuous Monitoring of Department of Defense Information Systems for Cybersecurity


“(a) In General.—The Secretary of Defense shall direct the Chief Information Officer of the Department of Defense to work, in coordination with the Chief Information Officers of the military departments and the Defense Agencies and with senior cybersecurity and information assurance officials within the Department of Defense and otherwise within the Federal Government, to achieve, to the extent practicable, the following:

“(1) The continuous prioritization of the policies, principles, standards, and guidelines developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) based upon the evolving threat of information security incidents with respect to national security systems, the vulnerability of such systems to such incidents, and the consequences of information security incidents involving such systems.

“(2) The automation of continuous monitoring of the effectiveness of the information security policies, procedures, and practices within the information infrastructure of the Department of Defense, and the compliance of that infrastructure with such policies, procedures, and practices, including automation of—

“(A) management, operational, and technical controls of every information system identified in the inventory required under section 3505 (c) of title 44, United States Code; and

“(B) management, operational, and technical controls relied on for evaluations under section 3545 of title 44, United States Code.

“(b) Definitions.—In this section:

“(1) The term ‘information security incident’ means an occurrence that—
“(A) actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information such system processes, stores, or transmits; or

“(B) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies with respect to an information system.

“(2) The term ‘information infrastructure’ means the underlying framework, equipment, and software that an information system and related assets rely on to process, transmit, receive, or store information electronically.

“(3) The term ‘national security system’ has the meaning given that term in section 3542 (b)(2) of title 44, United States Code.”