''(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

Pub. L. 111–383, div. A, title IX, §931, Jan. 7, 2011, 124 Stat. 4334, provided that:

''(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.''

§ 2223a. Information technology acquisition planning and oversight requirements

(a) ESTABLISHMENT OF PROGRAM.—The Secretary of Defense shall establish a program to improve the planning and oversight processes for the acquisition of major automated information systems by the Department of Defense.

(b) PROGRAM COMPONENTS.—The program established under subsection (a) shall include—

(1) a documented process for information technology acquisition planning, requirements development and management, project management and oversight, earned value management, and risk management;

(2) the development of appropriate metrics that can be implemented and monitored on a real-time basis for performance measurement of—

(A) processes and development status of investments in major automated information system programs;

(B) continuous process improvement of such programs; and

(C) achievement of program and investment outcomes;

(3) a process to ensure that key program personnel have an appropriate level of experience, training, and education in the planning, acquisition, execution, management, and oversight of information technology systems;

(4) a process to ensure sufficient resources and infrastructure capacity for test and evaluation of information technology systems;

(5) a process to ensure that military departments and Defense Agencies adhere to established processes and requirements relating to the planning, acquisition, execution, management, and oversight of information technology programs and developments; and

(6) a process under which an appropriate Department of Defense official may intervene or terminate the funding of an information technology investment if the investment is at risk of not achieving major project milestones.

(Added Pub. L. 111–383, div. A, title VIII, §805(a)(1), Jan. 7, 2011, 124 Stat. 4259.)

DATA SERVERS AND CENTERS

Pub. L. 112–81, div. B, title XXVIII, §2867, Dec. 31, 2011, 125 Stat. 1704, provided that:

''(a) LIMITATIONS ON OBLIGATION OF FUNDS.—

''(1) LIMITATIONS.—

''(A) BEFORE PERFORMANCE PLAN.—During the period beginning on the date of the enactment of this Act [Dec. 31, 2011] and ending on May 1, 2012, a department, agency, or component of the Department of Defense may not obligate funds for a data server farm or data center unless approved by the Chief Information Officer of the Department of Defense or the Chief Information Officer of a component of the Department to whom the Chief Information Officer of the Department has specifically delegated such approval authority.

''(B) UNDER PERFORMANCE PLAN.—After May 1, 2012, a department, agency, or component of the Department may not obligate funds for a data center, or any information systems technology used therein, unless that obligation is in accordance with the performance plan required by subsection (b) and is approved as described in subparagraph (A).

''(2) REQUIREMENTS FOR APPROVALS.—

''(A) BEFORE PERFORMANCE PLAN.—An approval of the obligation of funds may not be granted under paragraph (1)(A) unless the official granting the approval determines, in writing, that existing resources of the agency, component, or element concerned cannot affordably or practically be used or modified to meet the requirements to be met through the obligation of funds.

''(B) UNDER PERFORMANCE PLAN.—An approval of the obligation of funds may not be granted under paragraph (1)(B) unless the official granting the approval determines that—

''(i) existing resources of the Department do not meet the operation requirements to be met through the obligation of funds; and

''(ii) the proposed obligation is in accordance with the performance standards and measures established by the Chief Information Officer of the Department under subsection (b).

''(3) REPORTS.—Not later than 30 days after the end of each calendar quarter, each Chief Information Officer of a component of the Department who grants an approval under paragraph (1) during such calendar quarter shall submit to the Chief Information Officer of the Department a report on the approval or approvals so granted during such calendar quarter.

''(b) PERFORMANCE PLAN FOR REDUCTION OF RESOURCES REQUIRED FOR DATA SERVERS AND CENTERS.—

''(1) COMPONENT PLANS.—

''(A) IN GENERAL.—Not later than January 15, 2012, the Secretaries of the military departments and the heads of the Defense Agencies shall each submit to the Chief Information Officer of the Department a plan for the department or agency concerned to achieve the following:

''(i) A reduction in the square feet of floor space devoted to information systems technologies, attendant support technologies, and operations within data centers.

''(ii) A reduction in the use of all utilities necessary to power and cool information systems technologies and data centers.

''(iii) An increase in multi-organizational utilization of data centers, information systems technologies, and associated resources.

''(iv) A reduction in the investment for capital infrastructure or equipment required to support data centers as measured in cost per megawatt of data storage.

''(v) A reduction in the number of commercial and government developed applications running on data servers and within data centers.

''(vi) A reduction in the number of government and vendor provided full-time equivalent personnel, and in the cost of labor, associated with the operation of data servers and data centers.

''(B) SPECIFICATION OF REQUIRED ELEMENTS.—The Chief Information Officer of the Department shall specify the particular performance standards and measures and implementation elements to be included in the plans submitted under this paragraph, including specific goals and schedules for achieving the matters specified in subparagraph (A).

''(2) DEFENSE-WIDE PLAN.—

''(A) IN GENERAL.—Not later than April 1, 2012, the Chief Information Officer of the Department shall submit to the congressional defense committees [Committees on Armed Services and Appropriations of the Senate and the House of Representatives] a performance plan for a reduction in the resources required for data centers and information systems technologies Department-wide. The plan shall be based upon and incorporate appropriate elements of the plans submitted under paragraph (1).

''(B) ELEMENTS.—The performance plan required under this paragraph shall include the following:

''(i) A Department-wide performance plan for achieving the matters specified in paragraph (1)(A), including performance standards and measures for data centers and information systems technologies, goals and schedules for achieving such matters, and an estimate of cost savings anticipated through implementation of the plan.

''(ii) A Department-wide strategy for each of the following:

''(I) Desktop, laptop, and mobile device virtualization.

''(II) Transitioning to cloud computing.

''(III) Migration of Defense data and government-provided services from Department-owned and operated data centers to cloud computing services generally available within the private sector that provide a better capability at a lower cost with the same or greater degree of security.

''(IV) Utilization of private sector-managed security services for data centers and cloud computing services.

''(V) A finite set of metrics to accurately and transparently report on data center infrastructure (space, power and cooling): age, cost, capacity, usage, energy efficiency and utilization, accompanied with the aggregate data for each data center site in use by the Department in excess of 100 kilowatts of information technology power demand.

''(VI) Transitioning to just-in-time delivery of Department-owned data center infrastructure (space, power and cooling) through use of modular data center technology and integrated data center infrastructure management software.

''(3) RESPONSIBILITY.—The Chief Information Officer of the Department shall discharge the responsibility for establishing performance standards and measures for data centers and information systems technologies for purposes of this subsection. Such responsibility may not be delegated.

''(c) EXCEPTION.—The Chief Information Officer of the Department and the Chief Information Officer of the Intelligence Community may jointly exempt from the applicability of this section such intelligence components of the Department of Defense (and the programs and activities thereof) that are funded through the National Intelligence Program (NIP) as the Chief Information Officers consider appropriate.

''(d) REPORTS ON COST SAVINGS.—

''(1) IN GENERAL.—Not later than March 1 of each fiscal year, and ending in fiscal year 2016, the Chief Information Officer of the Department shall submit to the appropriate committees of Congress a report on the cost savings, cost reductions, cost avoidances, and performance gains achieved, and anticipated to be achieved, as of the date of such report as a result of activities undertaken under this section.

''(2) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this subsection, the term 'appropriate committees of Congress' means—

''(A) the Committee on Armed Services, the Committee on Appropriations, and the Select Committee on Intelligence of the Senate; and

''(B) the Committee on Armed Services, the Committee on Appropriations, and the Permanent Select Committee on Intelligence of the House of Representatives.''

§ 2224. Defense Information Assurance Program

(a) DEFENSE INFORMATION ASSURANCE PROGRAM.—The Secretary of Defense shall carry out a program, to be known as the ''Defense Information Assurance Program'', to protect and defend Department of Defense information, information systems, and information networks that are critical to the Department and the armed forces during day-to-day operations and operations in times of crisis.

(b) OBJECTIVES OF THE PROGRAM.—The objectives of the program shall be to provide continuously for the availability, integrity, authentication, confidentiality, nonrepudiation, and rapid restitution of information and information systems that are essential elements of the Defense Information Infrastructure.

(c) PROGRAM STRATEGY.—In carrying out the program, the Secretary shall develop a program strategy that encompasses those actions necessary to assure the readiness, reliability, continuity, and integrity of Defense information systems, networks, and infrastructure, including through compliance with subchapter II of chapter 35 of title 44, including through compliance with subchapter III of chapter 35 of title 44. The program strategy shall include the following:

(1) A vulnerability and threat assessment of elements of the defense and supporting nondefense information infrastructures that are essential to the operations of the Department and the armed forces.