DEPARTMENT OF DEFENSE
CHIEF INFORMATION OFFICER
DESK REFERENCE

VOLUME I
FOUNDATION DOCUMENTS

August 2006

Table of Contents

`

Editor's note: We have provided condensed versions of some of the laws, followed by their full texts.

Clinger Cohen Act of 1996, Title 40

U.S. Code	40 U.S.C. 1401 et seq.
Public Law	104-106, Division E
Date	February 10, 1996
Reports	U.S. House. Conference Report. H. Report 104-450[1]
URL	Division D – Federal Acquisition Reform Act of 1996 http://uscode.house.gov/download/title_40.shtml Division E – The Information Technology Management Reform Act of 1996 http://uscode.house.gov/download/title_40.shtml

Editor's note: The Information Technology Management Reform Act (ITMRA) (Division E) and the Federal Acquisition Reform Act (FARA) (Division D) were signed into law as part of the National Defense Authorization Act for Fiscal Year 1996. The ITMRA and FARA were subsequently designated the Clinger Cohen Act of 1996 (CCA), encompassing both. This is the first time in law that Chief Information Officers are established in government agencies, along with listing their roles and responsibilities. In addition, the ITMRA directs Federal agencies to focus more on the results achieved through IT investments while streamlining the Federal IT procurement process. Specifically, the ITMRA emphasizes rigor and structure in how agencies approach the selection and management of IT projects. FARA increases the discretion of contracting officers in an effort to promote efficient competition. FARA also permits the use of Simplified Acquisition Procedures in the acquisition of commercial items up to $5 million.

[1] An earlier version of the legislation (H.R. 1530/S. 1026) was vetoed by the President on December 22, 1995. U.S. House, Committee on National Security, H. Report No. 104-131; U.S. Senate, Committee on Armed Services, S. Report No. 104-112; U.S. House, Conference Report, H. Report No. 104-406

Information Technology Management Reform Act, Condensed[2]

The Office Management and Budget (OMB) Director is responsible for improving the acquisition, use, and disposal of information technology (IT) to improve Federal programs. OMB is to develop process for analyzing, tracking, and evaluating the risks and results of all major IT investments by Federal agencies. OMB shall evaluate the Information Resources Management (IRM) practices of executive agencies with respect to the performance and results of IT investments; and implement reviews of executive agency activities through the budget process. To enforce accountability for IRM and IT investments, OMB may (1) influence IRM budgets, (2) use administrative controls to restrict agency funds, and (3) designate an executive agent to contract out for agencies' IT management and acquisition.

Agency heads are to design and implement processes for maximizing the value and managing the risks of their IT acquisitions. This provides for the selection of investments using minimum criteria on whether to undertake an investment and gives a means for senior management to obtain timely information on cost, capability of the system to meet requirements, timeliness and quality. IT investment processes are to be integrated with the processes for making budget, financial, and program management decisions.

ITMRA establishes in law, Chief Information Officers (CIO) for Federal agencies. CIOs are responsible for providing advice and assistance to agency heads on IT acquisition and IRM. The CIO is responsible for developing, maintaining and facilitating the implementation of a sound and integrated IT architecture. The architecture is an integrated framework for evolving or maintaining existing IT and acquiring new IT. The agency heads shall identify in the agency's IRM plan (required by the Paperwork Reduction Act (PRA)), major IT acquisition programs that have significantly deviated from their respective cost, performance or schedule goals.

Agency heads shall ensure IT performance measurements are prescribed for acquisition and use and that they measure how well IT supports agency programs. CIOs are to monitor performance of IT programs, evaluate the performance of those programs based on

[2] Source: GAO

measures, and advise agency heads on continuing, modifying or terminating the programs or projects. Agency heads are to establish policies and procedures that (1) ensure information systems are designed, developed, maintained and used effectively; and (2) ensure program performance data are provided on a reliable, consistent and timely basis.

Federal Acquisition Reform Act, Condensed[3]

Section 4101, Efficient Competition. This provision makes no change to the Competition and Contracting Act. The Federal Acquisition Regulations (FAR) shall ensure that the requirement to obtain full and open competition is implemented in a manner that is consistent with the need to efficiently fulfill the Government's requirements.
Section 4102, Efficient Competitive Range Determinations. “The conferees intend that the determination of the competitive range be made after the initial evaluation of proposals, on the basis of the rating of those proposals. The rating shall be made on the basis of price, quality and other factors specified in the solicitation for the evaluation of proposals."[4]

Section 4201, Commercial Item Exception to Requirement for Certified Cost or Pricing Data. Submission of certified cost or pricing data shall not be required for the acquisition of a commercial item [this is a new exception]. The contracting officer is still authorized to require the submission of information other than certified cost or pricing data to determine price reasonableness.

Section 4202, Application of Simplified Procedures to Certain Commercial Items. Authorizes the establishment in the FAR of simplified procedures for acquisitions within a certain dollar range (not to exceed $5,000,000) when the contracting officer reasonably expects that offers will include only commercial items.

[3] Division D, Federal Acquisition Reform Act (FARA) of 1996. FARA provisions are based on H.R. 1670, which was introduced jointly on 5/18/95 by Rep. William Clinger, Chairman, Government Reform and Oversight Committee, and Rep. Floyd Spence, Chairman, National Security Committee, and which passed the full House 423-0 on 9/14/95.

[4] 1/22/96 Conference Report that accompanies S.1124

Clinger-Cohen Act of 1996

Short Title

This Act may be cited as the “National Defense Authorization Act for Fiscal Year 1996”.

TITLE 40 - PUBLIC BUILDINGS, PROPERTY, AND WORKS

TITLE 40 - SUBTITLE III - CHAPTER 111 - GENERAL

TITLE 40 - SUBTITLE III - CHAPTER 113 - RESPONSIBILITY FOR ACQUISITIONS OF INFORMATION TECHNOLOGY

TITLE 40 - SUBTITLE III - CHAPTER 113

TITLE 40 - SUBTITLE III - CHAPTER 117 - ADDITIONAL INFORMATION RESOURCES MANAGEMENT MATTERS

TITLE 40 - SUBTITLE III - CHAPTER 111

§ 11101. Definitions

In this subtitle, the following definitions apply:

(1) Commercial item.- The term "commercial item" has the meaning given that term in section 4 of the Office of Federal Procurement Policy Act (41 U.S.C. 403).

(2) Executive agency.- The term "executive agency" has the meaning given that term in section 4 of the Act (41 U.S.C. 403).

(3) Information resources.- The term "information resources" has the meaning given that term in section 3502 of title 44.

(4) Information resources management.- The term "information resources management" has the meaning given that term in section 3502 of title 44.

(5) Information system.- The term "information system" has the meaning given that term in section 3502 of title 44.

(6) Information technology.- The term "information technology"-

(A) with respect to an executive agency means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use –

(i) of that equipment; or

(ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(B) includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources; but

(C) does not include any equipment acquired by a federal contractor incidental to a federal contract.

TITLE 40 - SUBTITLE III - CHAPTER 111

§ 11102. Sense of Congress

It is the sense of Congress that, during the five-year period beginning with 1996, executive agencies should achieve each year through improvements in information resources management by the agency-

(1) at least a five percent decrease in the cost (in constant fiscal year 1996 dollars) incurred by the agency in operating and maintaining information technology; and

(2) a five percent increase in the efficiency of the agency operations.

TITLE 40 - SUBTITLE III - CHAPTER 111

§ 11103. Applicability to national security systems

(a) Definition.-

(1) National security system. - In this section, the term "national security system" means a telecommunications or information system operated by the Federal Government, the function, operation, or use of which –

(A) involves intelligence activities;
(B) involves cryptologic activities related to national security;
(C) involves command and control of military forces;
(D) involves equipment that is an integral part of a weapon or weapons system; or
(E) subject to paragraph (2), is critical to the direct fulfillment of military or intelligence missions.

(2) Limitation.- Paragraph (1)(E) does not include a system to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(b) In General.- Except as provided in subsection (c), chapter 113 of this title does not apply to national security systems.

(c) Exceptions.-

(1) In general.- Sections 11313, 11315, and 11316 of this title apply to national security systems.

(2) Capital planning and investment control.- The heads of executive agencies shall apply sections 11302 and 11312 of this title to national security systems to the extent practicable.

(3) Applicability of performance-based and results-based management to national security systems.

(A) In general.- Subject to subparagraph (B), the heads of executive agencies shall apply section 11303 of this title to national security systems to the extent practicable.

(B) Exception.-National security systems are subject to section 11303 (b)(5) of this title, except for subparagraph (B)(iv).

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER I -

§ 11301. Responsibility of Director

In fulfilling the responsibility to administer the functions assigned under chapter 35 of title 44, the Director of the Office of Management and Budget shall comply with this chapter with respect to the specific matters covered by this chapter.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER I -

§ 11302. Capital planning and investment control

(a) Federal Information Technology.- The Director of the Office of Management and Budget shall perform the responsibilities set forth in this section in fulfilling the responsibilities under section 3504 (h) of title 44.

(b) Use of Information Technology in Federal Programs - The Director shall promote and improve the acquisition, use, and disposal of information technology by the Federal Government to improve the productivity, efficiency, and effectiveness of federal programs, including through dissemination of public information and the reduction of information collection burdens on the public.

(c) Use of Budget Process -

(1) Analyzing, tracking, and evaluating capital investments.- As part of the budget process, the Director shall develop a process for analyzing, tracking, and evaluating the risks and results of all major capital investments made by an executive agency for information systems. The process shall cover

the life of each system and shall include explicit criteria for analyzing the projected and actual costs, benefits, and risks associated with the investments.

(2) Report to Congress.- At the same time that the President submits the budget for a fiscal year to Congress under section 1105 (a) of title 31, the Director shall submit to Congress a report on the net program performance benefits achieved as a result of major capital investments made by executive agencies for information systems and how the benefits relate to the accomplishment of the goals of the executive agencies.

(d) Information Technology Standards.-The Director shall oversee the development and implementation of standards and guidelines pertaining to federal computer systems by the Secretary of Commerce through the National Institute of Standards and Technology under section 11331 of this title and section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

(e) Designation of Executive Agents for Acquisitions - The Director shall designate the head of one or more executive agencies, as the Director considers appropriate, as executive agent for Government-wide acquisitions of information technology.

(f) Use of Best Practices in Acquisitions - The Director shall encourage the heads of the executive agencies to develop and use the best practices in the acquisition of information technology.

(g) Assessment of Other Models for Managing Information Technology - On a continuing basis, the Director shall assess the experiences of executive agencies, state and local governments, international organizations, and the private sector in managing information technology.

(h) Comparison of Agency Uses of Information Technology - The Director shall compare the performances of the executive agencies in using information technology and shall disseminate the comparisons to the heads of the executive agencies.

(i) Monitoring Training - The Director shall monitor the development and implementation of training in information resources management for executive agency personnel.

(j) Informing Congress - The Director shall keep Congress fully informed on the extent to which the executive agencies are improving the performance of agency programs and the accomplishment of the agency missions through the use of the best practices in information resources management.

(k) Coordination of Policy Development and Review - The Director shall coordinate with the Office of Federal Procurement Policy the development and review by the Administrator of the Office of Information and Regulatory Affairs of policy associated with federal acquisition of information technology.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER I -

§ 11303. Performance-based and results-based management

(a) In General.- The Director of the Office of Management and Budget shall encourage the use of performance-based and results-based management in fulfilling the responsibilities assigned under section 3504 (h) of title 44.

(b) Evaluation of Agency Programs and Investments.-

(1) Requirement.-The Director shall evaluate the information resources management practices of the executive agencies with respect to the performance and results of the investments made by the executive agencies in information technology.

(2) Direction for executive agency action. - The Director shall issue to the head of each executive agency clear and concise direction that the head of each agency shall -

(A) establish effective and efficient capital planning processes for selecting, managing, and evaluating the results of all of its major investments in information systems;

(B) determine, before making an investment in a new information system-

(i) whether the function to be supported by the system should be performed by the private sector and, if so, whether any component of the executive agency performing that function should be converted from a governmental organization to a private sector organization; or

(ii) whether the function should be performed by the executive agency and, if so, whether the function should be performed by a private sector source under contract or by executive agency personnel;

(C) analyze the missions of the executive agency and, based on the analysis, revise the executive agency's mission-related processes and administrative processes, as appropriate, before making significant

investments in information technology to be used in support of those missions; and

(D) ensure that the information security policies, procedures, and practices are adequate.

(3) Guidance for multiagency investments.- The direction issued under paragraph (2) shall include guidance for undertaking efficiently and effectively interagency and Federal Government-wide investments in information technology to improve the accomplishment of missions that are common to the executive agencies.

(4) Periodic reviews - The Director shall implement through the budget process periodic reviews of selected information resources management activities of the executive agencies to ascertain the efficiency and effectiveness of information technology in improving the performance of the executive agency and the accomplishment of the missions of the executive agency.

(5) Enforcement of accountability.-

(A) In general.- The Director may take any action that the Director considers appropriate, including an action involving the budgetary process or appropriations management process, to enforce accountability of the head of an executive agency for information resources management and for the investments made by the executive agency in information technology.

(B) Specific actions - Actions taken by the Director may include -

(i) recommending a reduction or an increase in the amount for information resources that the head of the executive agency proposes for the budget submitted to Congress under section 1105 (a) of title 31;

(ii) reducing or otherwise adjusting apportionments and reapportionments of appropriations for information resources;

(iii) using other administrative controls over appropriations to restrict the availability of amounts for information resources; and

(iv) designating for the executive agency an executive agent to contract with private sector sources for the performance of information resources management or the acquisition of information technology.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER II -

§ 11311. Responsibilities

In fulfilling the responsibilities assigned under chapter 35 of title 44, the head of each executive agency shall comply with this subchapter with respect to the specific matters covered by this subchapter.

§ 11312. Capital planning and investment control

(a) Design of Process. - In fulfilling the responsibilities assigned under section 3506 (h) of title 44, the head of each executive agency shall design and implement in the executive agency a process for maximizing the value, and assessing and managing the risks, of the information technology acquisitions of the executive agency.

(b) Content of Process.- The process of an executive agency shall -

(1) provide for the selection of information technology investments to be made by the executive agency, the management of those investments, and the evaluation of the results of those investments;

(2) be integrated with the processes for making budget, financial, and program management decisions in the executive agency;

(3) include minimum criteria to be applied in considering whether to undertake a particular investment in information systems, including criteria related to the quantitatively expressed projected net, risk-adjusted return on investment and specific quantitative and qualitative criteria for comparing and prioritizing alternative information systems investment projects;

(4) identify information systems investments that would result in shared benefits or costs for other federal agencies or state or local governments;

(5) identify quantifiable measurements for determining the net benefits and risks of a proposed investment; and

(6) provide the means for senior management personnel of the executive agency to obtain timely information regarding the progress of an investment in an information system, including a system of milestones for measuring progress, on an independently

verifiable basis, in terms of cost, capability of the system to meet specified requirements, timeliness, and quality.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER II -

§ 11313. Performance and results-based management

In fulfilling the responsibilities under section 3506 (h) of title 44, the head of an executive agency shall -

(1) establish goals for improving the efficiency and effectiveness of agency operations and, as appropriate, the delivery of services to the public through the effective use of information technology;

(2) prepare an annual report, to be included in the executive agency's budget submission to Congress, on the progress in achieving the goals;

(3) ensure that performance measurements -

(A) are prescribed for information technology used by, or to be acquired for, the executive agency; and

(B) measure how well the information technology supports programs of the executive agency;

(4) where comparable processes and organizations in the public or private sectors exist, quantitatively benchmark agency process performance against those processes in terms of cost, speed, productivity, and quality of outputs and outcomes;

(5) analyze the missions of the executive agency and, based on the analysis, revise the executive agency's mission-related processes and administrative processes as appropriate before making significant investments in information technology to be used in support of the performance of those missions; and

(6) ensure that the information security policies, procedures, and practices of the executive agency are adequate.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER II -

§ 11314. Authority to acquire and manage information technology

(a) In General.- The authority of the head of an executive agency to acquire information technology includes-

(1) acquiring information technology as authorized by law;

(2) making a contract that provides for multiagency acquisitions of information technology in accordance with guidance issued by the Director of the Office of Management and Budget; and

(3) if the Director finds that it would be advantageous for the Federal Government to do so, making a multiagency contract for procurement of commercial items of information technology that requires each executive agency covered by the contract, when procuring those items, to procure the items under that contract or to justify an alternative procurement of the items.

(b) FTS 2000 Program.— The Administrator of General Services shall continue to manage the FTS 2000 program, and to coordinate the follow-on to that program, for and with the advice of the heads of executive agencies.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER II -

§ 11315. Agency Chief Information Officer

(a) Definition.- In this section, the term "information technology architecture", with respect to an executive agency, means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals.

(b) General Responsibilities - The Chief Information Officer of an executive agency is responsible for -

(1) providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed for the executive agency in a manner that implements the policies and procedures of this subtitle, consistent with chapter 35 of title 44 and the priorities established by the head of the executive agency;

(2) developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency; and

(3) promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency.

(c) Duties and Qualifications.- The Chief Information Officer of an agency listed in section 901 (b) of title 31—

(1) has information resources management duties as that official's primary duty;

(2) monitors the performance of information technology programs of the agency, evaluates the performance of those programs on the basis of the applicable performance measurements, and advises the head of the agency regarding whether to continue, modify, or terminate a program or project; and

(3) annually, as part of the strategic planning and performance evaluation process required (subject to section 1117 of title 31) under section 306 of title 5 and sections 1105 (a)(28), 1115–1117, and 9703 (as added by section 5(a) of the Government Performance and Results Act of 1993 (Public Law 103–62, 107 Stat. 289)) of title 31-

(A) assesses the requirements established for agency personnel regarding knowledge and skill in information resources management and the adequacy of those requirements for facilitating the achievement of the performance goals established for information resources management;

(B) assesses the extent to which the positions and personnel at the executive level of the agency and the positions and personnel at management level of the agency below the executive level meet those requirements;

(C) develops strategies and specific plans for hiring, training, and professional development to rectify any deficiency in meeting those requirements; and

(D) reports to the head of the agency on the progress made in improving information resources management capability.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER II -

§ 11316. Accountability

The head of each executive agency, in consultation with the Chief Information Officer and the Chief Financial Officer of that executive agency (or, in the case of an executive agency without a chief financial officer, any comparable official), shall establish policies and procedures to ensure that

(1) the accounting, financial, asset management, and other information systems of the executive agency are designed, developed, maintained, and used effectively to provide financial or program performance data for financial statements of the executive agency;

(2) financial and related program performance data are provided on a reliable, consistent, and timely basis to executive agency financial management systems; and

(3) financial statements support -

(A) assessments and revisions of mission-related processes and administrative processes of the executive agency; and

(B) measurement of the performance of investments made by the agency in information systems.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER II -

§ 11317. Significant deviations

The head of each executive agency shall identify in the strategic information resources management plan required under section 3506 (b)(2) of title 44 any major information technology acquisition program, or any phase or increment of that program, that has significantly deviated from the cost, performance, or schedule goals established for the program.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER II -

§ 11318. Interagency support

The head of an executive agency may use amounts available to the agency for oversight, acquisition, and procurement of information technology to support jointly with other executive agencies the activities of interagency groups that are established to advise the Director of the Office of Management and Budget in carrying out the Director's

responsibilities under this chapter. The use of those amounts for that purpose is subject to requirements and limitations on uses and amounts that the Director may prescribe. The Director shall prescribe the requirements and limitations during the Director's review of the executive agency's proposed budget submitted to the Director by the head of the executive agency for purposes of section 1105 of title 31.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER III -

§ 11331. Responsibilities for Federal information systems standards

(a) Definition. In this section, the term "information security" has the meaning given that term in section 3532 (b)(1) of title 44.

(b) Requirement to Prescribe Standards. -

(1) In general.-

(A) Requirement.- Except as provided under paragraph (2), the Director of the Office of Management and Budget shall, on the basis of proposed standards developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–

(a) and in consultation with the Secretary of Homeland Security, promulgate information security standards pertaining to Federal information systems.

(B) Required standards. - Standards promulgated under subparagraph (A) shall include -

(i) standards that provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3 (b)); and

(ii) such standards that are otherwise necessary to improve the efficiency of operation or security of Federal information systems.

(C) Required standards binding.- Information security standards described under subparagraph (B) shall be compulsory and binding.

(2) Standards and guidelines for national security systems.- Standards and guidelines for national security systems, as defined under section 3532 (3) of title 44, shall be developed, promulgated, enforced, and overseen as otherwise authorized by law and as directed by the President.

(c) Application of More Stringent Standards.- The head of an agency may employ standards for the cost-effective information security for all operations and assets within or under the supervision of that agency that are more stringent than the standards promulgated by the Director under this section, if such standards -

(1) contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Director; and

(2) are otherwise consistent with policies and guidelines issued under section 3533 of title 44.

(d) Requirements Regarding Decisions by Director -

(1) Deadline.- The decision regarding the promulgation of any standard by the Director under subsection (b) shall occur not later than 6 months after the submission of the proposed standard to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

(2) Notice and comment.- A decision by the Director to significantly modify, or not promulgate, a proposed standard submitted to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), shall be made after the public is given an opportunity to comment on the Director's proposed decision.

TITLE 40 - SUBTITLE III - CHAPTER 113 - SUBCHAPTER III -

§ 11332. Repealed. Pub. L. 107–296, title X, § 1005(a)(1), Nov. 25, 2002, 116 Stat. 2272; Pub. L. 107–347, title III, § 305(a), Dec. 17, 2002, 116 Stat. 2960] Section, Pub. L. 107–217, Aug. 21, 2002, 116 Stat. 1244, related to Federal computer system security training and plan.

TITLE 40 - SUBTITLE III - CHAPTER 115 - SUBCHAPTER I -

§ 11501. Authority to conduct pilot program

(a) In General -

(1) Purpose - In consultation with the Administrator for the Office of Information and Regulatory Affairs, the Administrator for Federal Procurement Policy may conduct a pilot program pursuant to the requirements

of section 11521 of this title [1] to test alternative approaches for the acquisition of information technology by executive agencies.

(2) Multiagency, multi-activity conduct of each program.— Except as otherwise provided in this chapter, the pilot program conducted under this chapter shall be carried out in not more than two procuring activities in each of the executive agencies that are designated by the Administrator for Federal Procurement Policy in accordance with this chapter to carry out the pilot program. With the approval of the Administrator for Federal Procurement Policy, the head of each designated executive agency shall select the procuring activities of the executive agency that are to participate in the test and shall designate a procurement testing official who shall be responsible for the conduct and evaluation of the pilot program within the executive agency.

(b) Limitation on Amount.— The total amount obligated for contracts entered into under the pilot program conducted under this chapter may not exceed $375,000,000. The Administrator for Federal Procurement Policy shall monitor those contracts and ensure that contracts are not entered into in violation of this subsection.

(c) Period of Programs -

(1) In general.- Subject to paragraph (2), the pilot program may be carried out under this chapter for the period, not in excess of five years, the Administrator for Federal Procurement Policy determines is sufficient to establish reliable results.

(2) Continuing validity of contracts.- A contract entered into under the pilot program before the expiration of that program remains in effect according to the terms of the contract after the expiration of the program.

TITLE 40 - SUBTITLE III - CHAPTER 115 - SUBCHAPTER I -

§ 11502. Evaluation criteria and plans

(a) Measurable Test Criteria.- To the maximum extent practicable, the head of each executive agency conducting the pilot program under section 11501 of this title shall establish measurable criteria for evaluating the effects of the procedures or techniques to be tested under the program.

(b) Test Plan.- Before the pilot program may be conducted under section 11501 of this title, the Administrator for Federal Procurement

Policy shall submit to Congress a detailed test plan for the program, including a detailed description of the procedures to be used and a list of regulations that are to be waived.

TITLE 40 - SUBTITLE III - CHAPTER 115 - SUBCHAPTER I -

§ 11503. Report

(a) Requirement.— Not later than 180 days after the completion of the pilot program under this chapter, the Administrator for Federal Procurement Policy shall-

(1) submit to the Director of the Office of Management and Budget a report on the results and findings under the program; and

(2) provide a copy of the report to Congress.

(b) Content.- The report shall include

(1) a detailed description of the results of the program, as measured by the criteria established for the program; and

(2) a discussion of legislation that the Administrator recommends, or changes in regulations that the Administrator considers necessary, to improve overall information resources management in the Federal Government.

TITLE 40 - SUBTITLE III - CHAPTER 115 - SUBCHAPTER I -

§ 11504. Recommended legislation

If the Director of the Office of Management and Budget determines that the results and findings under the pilot program under this chapter indicate that legislation is necessary or desirable to improve the process for acquisition of information technology, the Director shall transmit the Director's recommendations for that legislation to Congress.

TITLE 40 - SUBTITLE III - CHAPTER 115 - SUBCHAPTER I -

§ 11505. Rule of construction

This chapter does not authorize the appropriation or obligation of amounts for the pilot program authorized under this chapter.

TITLE 40 - SUBTITLE III - CHAPTER 115 - SUBCHAPTER II -

§ 11521. Repealed. Pub. L. 107–347, title II, § 210(h)(1), Dec. 17, 2002, 116 Stat. 2938]

Section, Pub. L. 107–217, Aug. 21, 2002, 116 Stat. 1247, related to the share-in-savings pilot program.

TITLE 40 - SUBTITLE III - CHAPTER 115 - SUBCHAPTER II -

§ 11522. **Repealed. Pub.** L. 107–314, div. A, title VIII, § 825(b)(1), Dec. 2, 2002, 116 Stat. 2615]

Section, Pub. L. 107–217, Aug. 21, 2002, 116 Stat. 1247, related to a pilot program to test the feasibility of using solutions-based contracting for the acquisition of information technology. Subsequent to repeal, Pub. L. 107–347, title II, § 210(h)(3)(A), Dec. 17, 2002, 116 Stat. 2938, directed that this section be renumbered section 11521 of this title.

TITLE 40 - SUBTITLE III - CHAPTER 117 -

§ 11701. Identification of excess and surplus computer equipment

In accordance with chapter 5 of this title, the head of an executive agency shall maintain an inventory of all computer equipment under the control of that official that is excess or surplus property.

TITLE 40 - SUBTITLE III - CHAPTER 117 - § 11702

§ 11702. Index of certain information in information systems included in directory established under section 4101 of title 44

If in designing an information technology system pursuant to this subtitle, the head of an executive agency determines that a purpose of the system is to disseminate information to the public, then the head of that executive agency shall reasonably ensure that an index of information disseminated by the system is included in the directory created pursuant to section 4101 of title 44. This section does not authorize the dissemination of information to the public unless otherwise authorized.

TITLE 40 - SUBTITLE III - CHAPTER 117 - § 11703

§ 11703. Procurement procedures

To the maximum extent practicable, the Federal Acquisition Regulatory Council shall ensure that the process for acquisition of information technology is a simplified, clear, and understandable process that specifically addresses the management of risk, incremental acquisitions, and the need to incorporate commercial information technology in a timely manner.

Information Technology: Additional Responsibilities of Chief Information Officers

U.S. Code	Title 10, Sec 2223
Public Law	105-261
Date	October 1, 1998
URL	http://uscode.house.gov/download/pls/10C131.txt
Editor's note: This law directs the DoD CIO to be responsible for reviewing and providing recommendations to the Secretary on budget requests for IT and national security systems; interoperability of information technology and national security systems in the Department; and information technology and national security systems standards. It also directs the DoD CIO to provide for the elimination of duplicate information technology and national security systems.	

(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 11103 of title 40.

Paperwork Reduction Act

U.S. Code	44 U.S.C. 3501 et seq.
Public Law	104-13
Date	May 22, 1995
Reports	U.S. House. Committee on Government Reform. H. Report No. 104-37 U.S. Senate. Committee on Governmental Affairs. S. Report No. 104-8 U.S. House. Conference Report. H. Report No. 104-99
URL	http://uscode.house.gov/download/pls/44C35.txt
Editor's note: This Act requires agencies to use information resources to improve their operations and fulfill their missions. It provides direction on reducing the paperwork burden; minimizing the cost of information; and maximizing the utility of information collected, maintained, shared and disseminated. It also serves to improve the quality of Federal information; uniform information resources management (IRM) policies and practices; the dissemination of public information; privacy; IT acquisition; and the information collection review process. It is the "umbrella" IRM legislation for the Federal government -- other statutes elaborate on its goals.	

Paperwork Reduction Act, Condensed[5]

Agency program officials, in consultation with the Senior IRM Official (now Chief Information Officer (CIO)) and Chief Financial Officer (CFO) are to define program information needs and develop strategies, systems, and capabilities to meet those needs.

Each agency is to develop and maintain a strategic IRM plan to help accomplish agency missions. Each agency is to maintain an ongoing process to ensure that IRM operations and decisions are

[5] Source: GAO

integrated with organizational planning, budget, financial management, human resources management and program decisions.

Agencies are to establish goals for IRM to improve the productivity, efficiency, and effectiveness of agency operations, and methods for measuring progress in achieving the goals. Agencies are to maximize the value and assess and manage the risks of major information system initiatives through a process that (a) integrates budget, financial, and program management decisions and (b) is used to select, control, and evaluate the results of the initiatives. Also agencies are to maximize the value of major information systems initiatives and evaluate the results of such initiatives.

The OMB Director is to provide an annual report to Congress on the extent to which agencies have improved program performance and the accomplishment of agency missions through IRM.

Paperwork Reduction Act

An Act to further the goals of the Paperwork Reduction Act to have Federal agencies become more responsible and publicly accountable for reducing the burden of Federal paperwork on the public, and for other purposes.

Short Title. This Act may be cited as the **"Paperwork Reduction Act of 1995".**

Sec. 2. Coordination of Federal Information Policy.

Chapter 35 of title 44, United States Code, is amended to read as follows:

CHAPTER 35 -- COORDINATION OF FEDERAL INFORMATION POLICY

Sec. 3501. Purposes

The purposes of this chapter are to –

(1) minimize the paperwork burden for individuals, small businesses, educational and nonprofit institutions, Federal contractors, State, local

and tribal governments, and other persons resulting from the collection of information by or for the Federal Government;

(2) ensure the greatest possible public benefit from and maximize the utility of information created, collected, maintained, used, shared and disseminated by or for the Federal Government;

(3) coordinate, integrate, and to the extent practicable and appropriate, make uniform Federal information resources management policies and practices as a means to improve the productivity, efficiency, and effectiveness of Government programs, including the reduction of information collection burdens on the public and the improvement of service delivery to the public;

(4) improve the quality and use of Federal information to strengthen decision-making, accountability, and openness in Government and society;

(5) minimize the cost to the Federal Government of the creation, collection, maintenance, use, dissemination, and disposition of information;

(6) strengthen the partnership between the Federal Government and State, local, and tribal governments by minimizing the burden and maximizing the utility of information created, collected, maintained, used, disseminated, and retained by or for the Federal Government;

(7) provide for the dissemination of public information on a timely basis, on equitable terms, and in a manner that promotes the utility of the information to the public and makes effective use of information technology;

(8) ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including laws relating to

(A) privacy and confidentiality, including section 552a of title 5;

(B) security of information, including the Computer Security Act of 1987 (Public Law 100-235); and

(C) access to information, including section 552 of title 5;

(9) ensure the integrity, quality, and utility of the Federal statistical system;

(10) ensure that information technology is acquired, used, and managed to improve performance of agency missions, including the reduction of information collection burdens on the public; and

(11) improve the responsibility and accountability of the Office of Management and Budget and all other Federal agencies to Congress and to the public for implementing the information collection review process, information resources management, and related policies and guidelines established under this chapter.

§ 3502. Definitions

As used in this chapter –

(1) the term **"agency"** means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency, but does not include –

(A) the General Accounting Office;

(B) Federal Election Commission;

(C) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or

(D) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities;

(2) the term "burden" means time, effort, or financial resources expended by persons to generate, maintain, or provide information to or for a Federal agency, including the resources expended for –

(A) reviewing instructions;

(B) acquiring, installing, and utilizing technology and systems;

(C) adjusting the existing ways to comply with any previously applicable instructions and requirements;

(D) searching data sources;

(E) completing and reviewing the collection of information; and

(F) transmitting, or otherwise disclosing the information;

(3) the term "collection of information" –

(A) means the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or

opinions by or for an agency, regardless of form or format, calling for either –

(i) answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the United States; or

(ii) answers to questions posed to agencies, instrumentalities, or employees of the United States which are to be used for general statistical purposes; and

(B) shall not include a collection of information described under section 3518(c)(1);(4) the term "Director" means the Director of the Office of Management and Budget;

(5) the term "independent regulatory agency" means the Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Consumer Product Safety Commission, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Federal Energy Regulatory Commission, the Federal Housing Finance Board, the Federal Maritime Commission, the Federal Trade Commission, the Interstate Commerce Commission, the Mine Enforcement Safety and Health Review Commission, the National Labor Relations Board, the Nuclear Regulatory Commission, the Occupational Safety and Health Review Commission, the Postal Rate Commission, the Securities and Exchange Commission, and any other similar agency designated by statute as a Federal independent regulatory agency or commission;

(6) the term "information resources" means information and related resources, such as personnel, equipment, funds, and information technology;

(7) the term "information resources management" means the process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of information collection burdens on the public;

(8) the term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information;

(9) the term "information technology" has the same meaning as the term "automatic data processing equipment" as defined by section 111(a)(2) and

(3)(C) (i) through (v) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C759(a)(2) and (3)(C) (i) through (v));

(10) the term "person" means an individual, partnership, association, corporation, business trust, or legal representative, an organized group of individuals, a State, territorial, tribal, or local government or branch thereof, or a political subdivision of a State, territory, tribal, or local government or a branch of a political subdivision;

(11) the term "practical utility" means the ability of an agency to use information, particularly the capability to process such information in a timely and useful fashion;

(12) the term "public information" means any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public;

(13) the term "recordkeeping requirement" means a requirement imposed by or for an agency on persons to maintain specified records, including a requirement to --

(A) retain such records;

(B) notify third parties, the Federal Government, or the public of the existence of such records;

(C) disclose such records to third parties, the Federal Government, or the public; or

(D) report to third parties, the Federal Government, or the public regarding such records; and

(14) the term "penalty" includes the imposition by an agency or court of a fine or other punishment; a judgment for monetary damages or equitable relief; or the revocation, suspension, reduction, or denial of a license, privilege, right, grant, or benefit.

Sec. 3503. (*Note*: -- Establishment.) Office of Information and Regulatory Affairs

(a) There is established in the Office of Management and Budget an office to be known as the Office of Information and Regulatory Affairs.

(b) There shall be at the head of the Office an Administrator who shall be appointed by the President, by and with the advice and consent of the Senate. The Director shall delegate to the Administrator the

authority to administer all functions under this chapter, except that any such delegation shall not relieve the Director of responsibility for the administration of such functions. The Administrator shall serve as principal adviser to the Director on Federal information resources management policy.

Sec. 3504. Authority and Functions of Director

(a)(1) The Director shall oversee the use of information resources to improve the efficiency and effectiveness of governmental operations to serve agency missions, including burden reduction and service delivery to the public. In performing such oversight, the Director shall --

(A) develop, coordinate and oversee the implementation of Federal information resources management policies, principles, standards, and guidelines; and

(B) provide direction and oversee –

(i) the review and approval of the collection of information and the reduction of the information collection burden;

(ii) agency dissemination of and public access to information;

(iii) statistical activities;

(iv) records management activities;

(v) privacy, confidentiality, security, disclosure, and sharing of information; and

(vi) the acquisition and use of information technology.

(2) The authority of the Director under this chapter shall be exercised consistent with applicable law.

(b) With respect to general information resources management policy, the Director shall –

(1) develop and oversee the implementation of uniform information resources management policies, principles, standards, and guidelines;

(2) foster greater sharing, dissemination, and access to public information, including through –

(A) the use of the Government Information Locator Service; and

(B) the development and utilization of common standards for information collection, storage, processing and communication, including standards for security, interconnectivity and interoperability;

(3) initiate and review proposals for changes in legislation, regulations, and agency procedures to improve information resources management practices;

(4) oversee the development and implementation of best practices in information resources management, including training; and

(5) oversee agency integration of program and management functions with information resources management functions.

(c) With respect to the collection of information and the control of paperwork, the Director shall --

(1) review and approve proposed agency collections of information;

(2) coordinate the review of the collection of information associated with Federal procurement and acquisition by the Office of Information and Regulatory Affairs with the Office of Federal Procurement Policy, with particular emphasis on applying information technology to improve the efficiency and effectiveness of Federal procurement, acquisition and payment, and to reduce information collection burdens on the public;

(3) minimize the Federal information collection burden, with particular emphasis on those individuals and entities most adversely affected;

(4) maximize the practical utility of and public benefit from information collected by or for the Federal Government; and

(5) establish and oversee standards and guidelines by which agencies are to estimate the burden to comply with a proposed collection of information.

(d) With respect to information dissemination, the Director shall develop and oversee the implementation of policies, principles, standards, and guidelines to --

(1) apply to Federal agency dissemination of public information, regardless of the form or format in which such information is disseminated; and

(2) promote public access to public information and fulfill the purposes of this chapter, including through the effective use of information technology.

(f) ***Note:*** Records. With respect to records management, the Director shall --

(1) provide advice and assistance to the Archivist of the United States and the Administrator of General Services to promote coordination in the administration of chapters 29, 31, and 33 of this title with the information resources management policies, principles, standards, and guidelines established under this chapter;

(2) review compliance by agencies with –

(A) the requirements of chapters 29, 31, and 33 of this title; and

(B) ***Note:*** Regulations. regulations promulgated by the Archivist of the United States and the Administrator of General Services; and

(3) oversee the application of records management policies, principles, standards, and guidelines, including requirements for archiving information maintained in electronic format, in the planning and design of information systems.

(g) With respect to privacy and security, the Director shall --

(1) develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies;

(2) oversee and coordinate compliance with sections 552 and 552a of title 5, the Computer Security Act of 1987 (40 U.S.C.759 note), and related information management laws; and

(3) require Federal agencies, consistent with the Computer Security Act of 1987 (40 U.S.C.759 note), to identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency.

(h) With respect to Federal information technology, the Director shall --

(1) in consultation with the Director of the National Institute of Standards and Technology and the Administrator of General Services --

(A) develop and oversee the implementation of policies, principles, standards, and guidelines for information technology functions and activities of the Federal Government, including periodic evaluations of major information systems; and

(B) oversee the development and implementation of standards under section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C759(d));

(2) monitor the effectiveness of, and compliance with, directives issued under sections 110 and 111 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C.757 and 759);

(3) coordinate the development and review by the Office of Information and Regulatory Affairs of policy associated with Federal procurement and acquisition of information technology with the Office of Federal Procurement Policy;

(4) ensure, through the review of agency budget proposals, information resources management plans and other means –

(A) agency integration of information resources management plans, program plans and budgets for acquisition and use of information technology; and

(B) the efficiency and effectiveness of inter-agency information technology initiatives to improve agency performance and the accomplishment of agency missions; and

(5) promote the use of information technology by the Federal Government to improve the productivity, efficiency, and effectiveness of Federal programs, including through dissemination of public information and the reduction of information collection burdens on the public.

Sec. 3505. Assignment of Tasks and Deadlines

(a) In carrying out the functions under this chapter, the Director shall

(1) in consultation with agency heads, set an annual Governmentwide goal for the reduction of information collection burdens by at least 10 percent during each of fiscal years 1996 and 1997 and 5 percent during each of fiscal years 1998, 1999, 2000, and 2001, and set annual agency goals to --

(A) reduce information collection burdens imposed on the public that

(i) represent the maximum practicable opportunity in each agency; and

(ii) are consistent with improving agency management of the process for the review of collections of information established under section 3506(c); and

(B) improve information resources management in ways that increase the productivity, efficiency and effectiveness of Federal programs, including service delivery to the public;

(2) with selected agencies and non-Federal entities on a voluntary basis, conduct pilot projects to test alternative policies, practices, regulations, and procedures to fulfill the purposes of this chapter, particularly with regard to minimizing the Federal information collection burden; and

(3) in consultation with the Administrator of General Services, the Director of the National Institute of Standards and Technology, the Archivist of the United States, and the Director of the Office of Personnel Management, develop and maintain a Governmentwide strategic plan for information resources management, that shall include

(A) a description of the objectives and the means by which the Federal Government shall apply information resources to improve agency and program performance; (B) plans for –

(i) reducing information burdens on the public, including reducing such burdens through the elimination of duplication and meeting shared data needs with shared resources;

(ii) enhancing public access to and dissemination of, information, using electronic and other formats; and

(iii) meeting the information technology needs of the Federal Government in accordance with the purposes of this chapter; and

(C) a description of progress in applying information resources management to improve agency performance and the accomplishment of missions.

(b) For purposes of any pilot project conducted under subsection

(a)(2), the Director may, after consultation with the agency head, waive the application of any administrative directive issued by an agency with which the project is conducted, including any directive requiring a collection of information, after giving timely notice to the public and the Congress regarding the need for such waiver.

Sec. 3506. Federal Agency Responsibilities

(a)(1) The head of each agency shall be responsible for --

(A) carrying out the agency's information resources management activities to improve agency productivity, efficiency, and effectiveness; and

(B) complying with the requirements of this chapter and related policies established by the Director.

(2)(A) ***Note:*** Reports. Except as provided under subparagraph (B), the head of each agency shall designate a senior official who shall report directly to such agency head to carry out the responsibilities of the agency under this chapter.

(B) ***Note***: Reports. The Secretary of the Department of Defense and the Secretary of each military department may each designate senior officials who shall report directly to such Secretary to carry out the responsibilities of the department under this chapter. If more than one official is designated, the respective duties of the officials shall be clearly delineated.

(3) The senior official designated under paragraph (2) shall head an office responsible for ensuring agency compliance with and prompt, efficient, and effective implementation of the information policies and information resources management responsibilities established under this chapter, including the reduction of information collection burdens on the public. The senior official and employees of such office shall be selected with special attention to the professional qualifications required to administer the functions described under this chapter.

(4) Each agency program official shall be responsible and accountable for information resources assigned to and supporting the programs under such official. In consultation with the senior official designated under paragraph (2) and the agency Chief Financial Officer (or comparable official), each agency program official shall define program information needs and develop strategies, systems, and capabilities to meet those needs.

(b) With respect to general information resources management, each agency shall --

(1) manage information resources to –

(A) reduce information collection burdens on the public;

(B) increase program efficiency and effectiveness; and

(C) improve the integrity, quality, and utility of information to all users within and outside the agency, including capabilities for ensuring

dissemination of public information, public access to government information, and protections for privacy and security;

(2) in accordance with guidance by the Director, develop and maintain a strategic information resources management plan that shall describe how information resources management activities help accomplish agency missions;

(3) develop and maintain an ongoing process to –

(A) ensure that information resources management operations and decisions are integrated with organizational planning, budget, financial management, human resources management, and program decisions;

(B) in cooperation with the agency Chief Financial Officer (or comparable official), develop a full and accurate accounting of information technology expenditures, related expenses, and results; and

(C) establish goals for improving information resources management's contribution to program productivity, efficiency, and effectiveness, methods for measuring progress towards those goals, and clear roles and responsibilities for achieving those goals;

(4) in consultation with the Director, the Administrator of General Services, and the Archivist of the United States, maintain a current and complete inventory of the agency's information resources, including directories necessary to fulfill the requirements of section 3511 of this chapter; and

(5) in consultation with the Director and the Director of the Office of Personnel Management, conduct formal training programs to educate agency program and management officials about information resources management.

(c) With respect to the collection of information and the control of paperwork, each agency shall --

(1) establish a process within the office headed by the official designated under subsection (a), that is sufficiently independent of program responsibility to evaluate fairly whether proposed collections of information should be approved under this chapter, to --

(A) review each collection of information before submission to the Director for review under this chapter, including –

(i) an evaluation of the need for the collection of information;

(ii) a functional description of the information to be collected;

(iii) a plan for the collection of the information;

(iv) a specific, objectively supported estimate of burden;

(v) a test of the collection of information through a pilot program, if appropriate; and

(vi) a plan for the efficient and effective management and use of the information to be collected, including necessary resources;

(B) ensure that each information collection –

(i) is inventoried, displays a control number and, if appropriate, an expiration date;

(ii) indicates the collection is in accordance with the clearance requirements of section 3507; and

(iii) informs the person receiving the collection of information of –

(I) the reasons the information is being collected;

(II) the way such information is to be used;

(III) an estimate, to the extent practicable, of the burden of the collection;

(IV) whether responses to the collection of information are voluntary, required to obtain a benefit, or mandatory; and

(V) the fact that an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number; and

(C) assess the information collection burden of proposed legislation affecting the agency;

(2)(A) ***Note:*** Federal Register, publication. except as provided under subparagraph (B) or section 3507(j), provide 60-day notice in the Federal Register, and otherwise consult with members of the public and affected agencies concerning each proposed collection of information, to solicit comment to –

(i) evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility;

(ii) evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information;

(iii) enhance the quality, utility, and clarity of the information to be collected; and

(iv) minimize the burden of the collection of information on those who are to respond, including information technology; and

(B) ***Note:*** Regulations. for any proposed collection of information contained in a proposed rule (to be reviewed by the Director under section 3507(d)), provide notice and comment through the notice of proposed rulemaking for the proposed rule and such notice shall have the same purposes specified under subparagraph (A) (i) through (iv); and

(3) certify (and provide a record supporting such certification, including public comments received by the agency) that each collection of information submitted to the Director for review under section 3507 –

(A) is necessary for the proper performance of the functions of the agency, including that the information has practical utility;

(B) is not unnecessarily duplicative of information otherwise reasonably accessible to the agency;

(C) reduces to the extent practicable and appropriate the burden on persons who shall provide information to or for the agency, including with respect to small entities, as defined under section 601(6) of title 5, the use of such techniques as –

(i) establishing differing compliance or reporting requirements or timetables that take into account the resources available to those who are to respond;

(ii) the clarification, consolidation, or simplification of compliance and reporting requirements; or

(iii) an exemption from coverage of the collection of information, or any part thereof;

(D) is written using plain, coherent, and unambiguous terminology and is understandable to those who are to respond;

(E) is to be implemented in ways consistent and compatible, to the maximum extent practicable, with the existing reporting and recordkeeping practices of those who are to respond;

(F) indicates for each recordkeeping requirement the length of time persons are required to maintain the records specified;

(G) contains the statement required under paragraph (1)(B)(iii);

(H) has been developed by an office that has planned and allocated resources for the efficient and effective management and use of the information to be collected, including the processing of the information in a manner which shall enhance, where appropriate, the utility of the information to agencies and the public;

(I) uses effective and efficient statistical survey methodology appropriate to the purpose for which the information is to be collected; and

(J) to the maximum extent practicable, uses information technology to reduce burden and improve data quality, agency efficiency and responsiveness to the public.

(d) ***Note:*** Public information. With respect to information dissemination, each agency shall --

(1) ensure that the public has timely and equitable access to the agency's public information, including ensuring such access through –

(A) encouraging a diversity of public and private sources for information based on government public information;

(B) in cases in which the agency provides public information maintained in electronic format, providing timely and equitable access to the underlying data (in whole or in part); and

(C) agency dissemination of public information in an efficient, effective, and economical manner;

(2) regularly solicit and consider public input on the agency's information dissemination activities;

(3) provide adequate notice when initiating, substantially modifying, or terminating significant information dissemination products; and

(4) not, except where specifically authorized by statute –

(A) establish an exclusive, restricted, or other distribution arrangement that interferes with timely and equitable availability of public information to the public;

(B) restrict or regulate the use, resale, or redissemination of public information by the public;

(C) charge fees or royalties for resale or redissemination of public information; or

(D) establish user fees for public information that exceed the cost of dissemination.

(e) With respect to statistical policy and coordination, each agency shall -

(1) ensure the relevance, accuracy, timeliness, integrity, and objectivity of information collected or created for statistical purposes;

(2) inform respondents fully and accurately about the sponsors, purposes, and uses of statistical surveys and studies;

(3) protect respondents" privacy and ensure that disclosure policies fully honor pledges of confidentiality;

(4) observe Federal standards and practices for data collection, analysis, documentation, sharing, and dissemination of information;

(5) ensure the timely publication of the results of statistical surveys and studies, including information about the quality and limitations of the surveys and studies; and

(6) make data available to statistical agencies and readily accessible to the public.

(f) ***Note:*** Records. With respect to records management, each agency shall implement and enforce applicable policies and procedures, including requirements for archiving information maintained in electronic format, particularly in the planning, design and operation of information systems.

(g) ***Note:*** Privacy. Computer technology. With respect to privacy and security, each agency shall --

(1) implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for the agency;

(2) assume responsibility and accountability for compliance 5, the Computer Security Act of 1987 (40 U.S.C759 note), and related information management laws; and

(3) consistent with the Computer Security Act of 1987 (40 U.S.C.759 note), identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency.

(h) ***Note:*** Science and technology. With respect to Federal information technology, each agency shall --

(1) implement and enforce applicable Governmentwide and agency information technology management policies, principles, standards, and guidelines;

(2) assume responsibility and accountability for information technology investments; with and coordinated management of sections 552 and 552a of title

(3) promote the use of information technology by the agency to improve the productivity, efficiency, and effectiveness of agency programs, including the reduction of information collection burdens on the public and improved dissemination of public information;

(4) propose changes in legislation, regulations, and agency procedures to improve information technology practices, including changes that improve the ability of the agency to use technology to reduce burden; and

(5) assume responsibility for maximizing the value and assessing and managing the risks of major information systems initiatives through a process that is –

(A) integrated with budget, financial, and program management decisions; and

(B) used to select, control, and evaluate the results of major information systems initiatives.

Sec. 3507. Public Information Collection Activities; Submission to Director; Approval and Delegation

(a) An agency shall not conduct or sponsor the collection of information unless in advance of the adoption or revision of the collection of information -

(1) the agency has --

(A) conducted the review established under section 3506(c)(1);

(B) evaluated the public comments received under section 3506(c)(2);

(C) submitted to the Director the certification required under section 3506(c)(3), the proposed collection of information, copies of pertinent statutory authority, regulations, and other related materials as the Director may specify; and

(D) ***Note:*** Federal Register, publication. published a notice in the Federal Register –

(i) stating that the agency has made such submission; and

(ii) setting forth –

(I) a title for the collection of information;

(II) a summary of the collection of information;

(III) a brief description of the need for the information and the proposed use of the information;

(IV) a description of the likely respondents and proposed frequency of response to the collection of information;

(V) an estimate of the burden that shall result from the collection of information; and

(VI) notice that comments may be submitted to the agency and Director;

(2) the Director has approved the proposed collection of information or approval has been inferred, under the provisions of this section; and

(3) the agency has obtained from the Director a control number to be displayed upon the collection of information.

(b) The Director shall provide at least 30 days for public comment prior to making a decision under subsection (c), (d), or (h), except as provided under subsection (j).

(c)(1) For any proposed collection of information not contained in a proposed rule, the Director shall notify the agency involved of the decision to approve or disapprove the proposed collection of information.

(2) The Director shall provide the notification under paragraph (1), within 60 days after receipt or publication of the notice under subsection (a)(1)(D), whichever is later.

(3) If the Director does not notify the agency of a denial or approval within the 60-day period described under paragraph (2) --

(A) the approval may be inferred;

(B) a control number shall be assigned without further delay; and

(C) the agency may collect the information for not more than 1 year.

(d)(1) ***Note****:* Proposed rule. For any proposed collection of information contained in a proposed rule --

(A) as soon as practicable, but no later than the date of publication of a notice of proposed rulemaking in the Federal Register, each agency shall forward to the Director a copy of any proposed rule which contains a collection of information and any information requested by the Director necessary to make the determination required under this subsection; and

(B) ***Note:*** Federal Register, publication. within 60 days after the notice of proposed rulemaking is published in the Federal Register, the Director may file public comments pursuant to the standards set forth in section 3508 on the collection of information contained in the proposed rule;

(2) ***Note:*** Regulations. Federal Register, publication. When a final rule is published in the Federal Register, the agency shall explain --

(A) how any collection of information contained in the final rule responds to the comments, if any, filed by the Director or the public; or

(B) the reasons such comments were rejected.

(3) If the Director has received notice and failed to comment on an agency rule within 60 days after the notice of proposed rulemaking, the Director may not disapprove any collection of information specifically contained in an agency rule.

(4) No provision in this section shall be construed to prevent the Director, in the Director's discretion –

(A) from disapproving any collection of information which was not specifically required by an agency rule;

(B) from disapproving any collection of information contained in an agency rule, if the agency failed to comply with the requirements of paragraph (1) of this subsection;

(C) from disapproving any collection of information contained in a final agency rule, if the Director finds within 60 days after the publication of the final rule that the agency's response to the Director's comments filed under paragraph (2) of this subsection was unreasonable; or

(D) from disapproving any collection of information contained in a final rule, if –

(i) the Director determines that the agency has substantially modified in the final rule the collection of information contained in the proposed rule; and

(ii) the agency has not given the Director the information required under paragraph (1) with respect to the modified collection of information, at least 60 days before the issuance of the final rule.

(5) This subsection shall apply only when an agency publishes a notice of proposed rulemaking and requests public comments.

(6) The decision by the Director to approve or not act upon a collection of information contained in an agency rule shall not be subject to judicial review.

(e)(1) Any decision by the Director under subsection (c), (d), (h), or

(j) to disapprove a collection of information, or to instruct the agency to make substantive or material change to a collection of information, shall be publicly available and include an explanation of the reasons for such decision.

(2) Any written communication between the Administrator of the Office of Information and Regulatory Affairs, or any employee of the Office of Information and Regulatory Affairs, and an agency or person not employed by the Federal Government concerning a proposed collection of information shall be made available to the public.

(3) This subsection shall not require the disclosure of --

(A) any information which is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; or

(B) any communication relating to a collection of information which is not approved under this chapter, the disclosure of which could lead to retaliation or discrimination against the communicator.

(f)(1) An independent regulatory agency which is administered by 2 or more members of a commission, board, or similar body, may by majority vote void

(A) any disapproval by the Director, in whole or in part, of a proposed collection of information of that agency; or

(B) an exercise of authority under subsection (d) of section 3507 concerning that agency.

(2) The agency shall certify each vote to void such disapproval or exercise to the Director, and explain the reasons for such vote. The Director shall without further delay assign a control number to such collection of information, and such vote to void the disapproval or exercise shall be valid for a period of 3 years.

(g) The Director may not approve a collection of information for a period in excess of 3 years.

(h)(1) If an agency decides to seek extension of the Director's approval granted for a currently approved collection of information, the agency shall --

(A) conduct the review established under section 3506(c), including the seeking of comment from the public on the continued need for, and burden imposed by the collection of information; and

(B) after having made a reasonable effort to seek public comment, but no later than 60 days before the expiration date of the control number assigned by the Director for the currently approved collection of information, submit the collection of information for review and approval under this section, which shall include an explanation of how the agency has used the information that it has collected.

(2) If under the provisions of this section, the Director disapproves a collection of information contained in an existing rule, or recommends or instructs the agency to make a substantive or material change to a collection of information contained in an existing rule, the Director shall

(A) ***Note:*** Federal Register, publication. Publish an explanation thereof in the Federal Register; and

(B) instruct the agency to undertake a rulemaking within a reasonable time limited to consideration of changes to the collection of information contained in the rule and thereafter to submit the collection of information for approval or disapproval under this chapter.

(3) An agency may not make a substantive or material modification to a collection of information after such collection has been approved by the Director, unless the modification has been submitted to the Director for review and approval under this chapter.

(i)(1) If the Director finds that a senior official of an agency designated under section 3506(a) is sufficiently independent of program responsibility to evaluate fairly whether proposed collections of information should be approved and has sufficient resources to carry out this responsibility effectively, the Director may, by rule in accordance with the notice and comment provisions of chapter 5 of title 5, United States Code, delegate to such official the authority to approve proposed collections of information in specific program areas, for specific purposes, or for all agency purposes.

(2) A delegation by the Director under this section shall not preclude the Director from reviewing individual collections of information if the Director determines that circumstances warrant such a review. The Director shall retain authority to revoke such delegations, both in general and with regard to any specific matter. In acting for the Director, any official to whom approval authority has been delegated under this section shall comply fully with the rules and regulations promulgated by the Director.

(j)(1) The agency head may request the Director to authorize a collection of information, if an agency head determines that --

(A) a collection of information –

(i) is needed prior to the expiration of time periods established under this chapter; and

(ii) is essential to the mission of the agency; and

(B) the agency cannot reasonably comply with the provisions of this chapter because –

(i) public harm is reasonably likely to result if normal clearance procedures are followed;

(ii) an unanticipated event has occurred; or

(iii) the use of normal clearance procedures is reasonably likely to prevent or disrupt the collection of information or is reasonably likely to cause a statutory or court ordered deadline to be missed.

(2) The Director shall approve or disapprove any such authorization request within the time requested by the agency head and, if approved, shall assign the collection of information a control number. Any collection of information conducted under this subsection may be conducted without compliance with the provisions of this chapter for a maximum of 90 days after the date on which the Director received the request to authorize such collection.

Sec. 3508. Determination of Necessity for Information; Hearing

Before approving a proposed collection of information, the Director shall determine whether the collection of information by the agency is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility. Before making a determination the Director may give the agency and other interested persons an opportunity to be heard or to submit statements in writing. To the extent, if any, that the Director determines that the collection of information by an agency is unnecessary for any reason, the agency may not engage in the collection of information.

Sec. 3509. Designation of Central Collection Agency

The Director may designate a central collection agency to obtain information for two or more agencies if the Director determines that the needs of such agencies for information will be adequately served by a single collection agency, and such sharing of data is not inconsistent with applicable law. In such cases the Director shall prescribe (with reference to the collection of information) the duties and functions of the collection agency so designated and of the agencies for which it is to act as agent (including reimbursement for costs). While the designation is in effect, an agency covered by the designation may not obtain for itself information for the agency which is the duty of the collection agency to obtain. The Director may modify the designation from time to time as circumstances require. The authority to designate under this section is subject to the provisions of section 3507(f) of this chapter.

Sec. 3510. Cooperation of Agencies in Making Information Available

(a) The Director may direct an agency to make available to another agency, or an agency may make available to another agency, information obtained by a collection of information if the disclosure is not inconsistent with applicable law.

(b)(1) If information obtained by an agency is released by that agency to another agency, all the provisions of law (including penalties) that relate to the unlawful disclosure of information apply to the officers and employees of the agency to which information is released to the same extent and in the same manner as the provisions apply to the officers and employees of the agency which originally obtained the information.

(2) The officers and employees of the agency to which the information is released, in addition, shall be subject to the same provisions of law, including penalties, relating to the unlawful disclosure of information as if the information had been collected directly by that agency.

Sec. 3511. Establishment and Operation of Government Information Locator Service

(a) In order to assist agencies and the public in locating information and to promote information sharing and equitable access by the public, the Director shall –

(1) cause to be established and maintained a distributed agency-based electronic Government Information Locator Service (hereafter in this section referred to as the "Service'), which shall identify the major information systems, holdings, and dissemination products of each agency;

(2) require each agency to establish and maintain an agency information locator service as a component of, and to support the establishment and operation of the Service;

(3) ***Note:*** Establishment. in cooperation with the Archivist of the United States, the Administrator of General Services, the Public Printer, and the Librarian of Congress, establish an interagency committee to advise the Secretary of Commerce on the development of technical standards for the Service to ensure compatibility, promote information sharing, and uniform access by the public;

(4) consider public access and other user needs in the establishment and operation of the Service;

(5) ensure the security and integrity of the Service, including measures to ensure that only information which is intended to be disclosed to the public is disclosed through the Service; and

(6) periodically review the development and effectiveness of the Service and make recommendations for improvement, including other mechanisms for improving public access to Federal agency public information.

(b) This section shall not apply to operational files as defined by the Central Intelligence Agency Information Act (50 U.S.C. 431 et seq.).

Sec. 3512. Public Protection

(a) Notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information that is subject to this chapter if --

(1) the collection of information does not display a valid control number assigned by the Director in accordance with this chapter; or

(2) the agency fails to inform the person who is to respond to the collection of information that such person is not required to respond to the collection of information unless it displays a valid control number.

(b) The protection provided by this section may be raised in the form of a complete defense, bar, or otherwise at any time during the agency administrative process or judicial action applicable there to.

Sec. 3513. Director Review of Agency Activities; Reporting; Agency Response

(a) In consultation with the Administrator of General Services, the Archivist of the United States, the Director of the National Institute of Standards and Technology, and the Director of the Office of Personnel Management, the Director shall periodically review selected agency information resources management activities to ascertain the efficiency and effectiveness of such activities to improve agency performance and the accomplishment of agency missions.

(b) Each agency having an activity reviewed under subsection (a) shall, within 60 days after receipt of a report on the review, provide a written plan to the Director describing steps (including milestones) to --

(1) be taken to address information resources management problems identified in the report; and

(2) improve agency performance and the accomplishment of agency missions.

Sec. 3514. Responsiveness to Congress

(a)(1) The Director shall --

(A) keep the Congress and congressional committees fully and currently informed of the major activities under this chapter; and

(B) ***Note:*** Reports. submit a report on such activities to the President of the Senate and the Speaker of the House of Representatives annually and at such other times as the Director determines necessary.

(2) The Director shall include in any such report a description of the extent to which agencies have -

(A) reduced information collection burdens on the public, including

(i) a summary of accomplishments and planned initiatives to reduce collection of information burdens;

(ii) a list of all violations of this chapter and of any rules, guidelines, policies, and procedures issued pursuant to this chapter;

(iii) a list of any increase in the collection of information burden, including the authority for each such collection; and

(iv) a list of agencies that in the preceding year did not reduce information collection burdens in accordance with section 3505(a)(1), a list of the programs and statutory responsibilities of those agencies that precluded that reduction, and recommendations to assist those agencies to reduce information collection burdens in accordance with that section;

(B) improved the quality and utility of statistical information;

(C) improved public access to Government information; and

(D) improved program performance and the accomplishment of agency missions through information resources management.

(b) The preparation of any report required by this section shall be based on performance results reported by the agencies and shall not increase the collection of information burden on persons outside the Federal Government.

Sec. 3515. Administrative Powers

Upon the request of the Director, each agency (other than an independent regulatory agency) shall, to the extent practicable, make its services, personnel, and facilities available to the Director for the performance of functions under this chapter.

Sec. 3516. Rules and Regulations

The Director shall promulgate rules, regulations, or procedures necessary to exercise the authority provided by this chapter.

Sec. 3517. Consultation With Other Agencies and the Public

(a) In developing information resources management policies, plans, rules, regulations, procedures, and guidelines and in reviewing collections of information, the Director shall provide interested agencies and persons early and meaningful opportunity to comment.

(b) Any person may request the Director to review any collection of information conducted by or for an agency to determine, if, under this chapter, a person shall maintain, provide, or disclose the information to or for the agency. Unless the request is frivolous, the Director shall, in coordination with the agency responsible for the collection of information

(1) respond to the request within 60 days after receiving the request, unless such period is extended by the Director to a specified date and the person making the request is given notice of such extension; and

(2) take appropriate remedial action, if necessary.

Sec. 3518. Effect on Existing Laws and Regulations

(a) Except as otherwise provided in this chapter, the authority of an agency under any other law to prescribe policies, rules, regulations, and procedures for Federal information resources management activities is subject to the authority of the Director under this chapter.

(b) Nothing in this chapter shall be deemed to affect or reduce the authority of the Secretary of Commerce or the Director of the Office of Management and Budget pursuant to Reorganization Plan No. 1 of 1977 (as amended) and Executive order, relating to telecommunications and information policy, procurement and management of telecommunications and information systems, spectrum use, and related matters.

(c)(1) Except as provided in paragraph (2), this chapter shall not apply to the collection of information --

(A) during the conduct of a Federal criminal investigation or prosecution, or during the disposition of a particular criminal matter;

(B) during the conduct of –

(i) a civil action to which the United States or any official or agency thereof is a party; or

(ii) an administrative action or investigation involving an agency against specific individuals or entities;

(C) by compulsory process pursuant to the Antitrust Civil Process Act and section 13 of the Federal Trade Commission Improvements Act of 1980; or

(D) during the conduct of intelligence activities as defined in section 3.4(e) of Executive Order No. 12333, issued December 4, 1981, or successor orders, or during the conduct of cryptologic activities that are communications security activities.

(2) This chapter applies to the collection of information during the conduct of general investigations (other than information collected in an antitrust investigation to the extent provided in subparagraph (C) of paragraph (1)) undertaken with reference to a category of individuals or entities such as a class of licensees or an entire industry.

(d) Nothing in this chapter shall be interpreted as increasing or decreasing the authority conferred by Public Law 89-306 on the Administrator of the General Services Administration, the Secretary of Commerce, or the Director of the Office of Management and Budget.

(e) Nothing in this chapter shall be interpreted as increasing or decreasing the authority of the President, the Office of Management and Budget or the Director thereof, under the laws of the United States, with respect to the substantive policies and programs of departments, agencies and offices, including the substantive authority of any Federal agency to enforce the civil rights laws.

Sec. 3519. Access to Information

Under the conditions and procedures prescribed in section 716 of title 31, the Director and personnel in the Office of Information and Regulatory Affairs

shall furnish such information as the Comptroller General may require for the discharge of the responsibilities of the Comptroller General. For the purpose of obtaining such information, the Comptroller General or representatives thereof shall have access to all books, documents, papers and records, regardless of form or format, of the Office.

Sec. 4. *Note:* 44 USC 3501 *Note*. Effective Date.

(a) In General. -- Except as otherwise provided in this section, this Act and the amendments made by this Act shall take effect on October 1.

E-Government Act of 2002

U.S. Code	44 U.S.C 101, Ch. 35 and 36
Public Law	107-347
Date	December 17, 2002
Committee Reports	U.S. House Conference Report 107-787 U.S. House. Committee on Government Reform. H. Report No. 107-787, Part 1 accompanying H.R. 2458 U.S. Senate. Committee on Governmental Affairs. S.
URL	http://cfr.law.cornell.edu/uscode/html/uscode44/usc_sup_01_44_10_35.html http://uscode.house.gov/download/pls/44C35.txt http://cfr.law.cornell.edu/uscode/html/uscode44/usc_sup_01_44_10_36.html http://uscode.house.gov/download/pls/44C36.txt
Editor's note: This Act enhances the management and promotion of electronic government (e-government) by establishing a Federal Administrator for e-government in the Office of Management and Budget (OMB), and a broad framework of measures that requires using Internet-based IT to enhance access to government information and services. It also defines e-government and statutorily authorizes the CIO Council.. The Act includes the Federal Information Security Management Act (FISMA) which provides for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. Non CIO-related sections of the E-Government Act of 2002 have been removed.	

E-Government Act[6], Condensed

Title I: OMB Electronic Government Service

Establishes an OMB Office of Electronic Government, headed by an Administrator appointed by the President. Requires the Administrator and other OMB officials to

---

[6] Source: Congressional Research Service

- Set the strategic direction for implementing electronic government
- Recommend changes relating to government-wide strategies and priorities for E-Government
- Promote innovative uses of IT by agencies
- Oversee distribution of funds from the E-Government Fund
- Lead the activities of the CIO Council
- Assist in establishing policies that set the framework for government IT standards developed by the National Institute of Standards and Technology (NIST) and promulgated by the Secretary of Commerce
- Coordinate with the Administrator for Federal Procurement Policy to ensure effective implementation of electronic procurement initiatives

This Act codifies Executive Order 13011 (Federal Information Technology) establishing the CIO Council and designating it as the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of Federal government information resources. Establishes the E-Government Fund to support relevant projects.

Title II: Federal Management and Promotion of Electronic Government Services

Each agency CIO is responsible for monitoring the implementation of IT standards, including common standards for interconnectivity and interoperability, categorization of government electronic information, and computer system efficiency and security.

Requires each agency to submit an annual E-Government status report.

Makes this title inapplicable to national security systems, with exceptions. Requires each agency to ensure that its methods for use and acceptance of electronic signatures are compatible with the relevant

policies and procedures issued by OMB.

Establishes the Interagency Committee on Government Information which is required to submit recommendations to OMB on the adoption of standards to enable the organization and categorization of government information. Requires OMB to promulgate guidance for agency websites.

Requires the Director of the Office of Personnel Management (OPM) to analyze IT and IRM personnel needs of the government and oversee the training needs of Federal employees in IT disciplines. Requires each agency head to establish and operate IT training programs.

Sets forth provisions regarding CIO authorities and responsibilities, IT training reporting, authority to detail employees to non-federal employers, and employee participation. Authorizes an agency head to arrange for the assignment of an agency employee who works in the IT management field to a private sector organization or of an employee of such an organization to the agency.

Directs the Administrator to study the use of IT to enhance crisis preparedness, response, and consequence management of natural and manmade disasters; and work with other agencies and local governments on pilot projects or reports to Congress.

Requires the Administrator to facilitate the development of common protocols for the development, acquisition, maintenance, distribution, and application of geographic information.

Title III: Information Security - FISMA

Requires Federal agencies to have agency-wide Information Security (IS) programs and report annually to OMB, the Comptroller General and Congress on the adequacy and effectiveness of IS policies, procedures and practices.

Sets forth provisions regarding delegation of the Director's authority regarding certain systems operated by the Department of Defense and by the Central Intelligence Agency.

Directs the head of each agency to delegate to the agency CIO the authority to ensure compliance with this Act and ensure that the agency has trained IS personnel.

Requires each agency to address in its annual IS report, adequacy and effectiveness in plans and reports relating to annual agency budgets, information resources management, IT management, program performance, financial management, financial management systems, and internal accounting and administrative controls; and report any significant deficiency.

Sets forth requirements regarding performance plans, and public notice and comment. Requires OMB to ensure the operation of a central Federal information security incident center. Requires each agency exercising control of a national security system to share information about information security incidents, threats, and vulnerabilities with the center to the extent consistent with standards and guidelines for national security systems.

Amends the National Institute of Standards and Technology Act to provide that NIST shall: (1) have the mission of developing standards, guidelines, and associated methods and techniques for information systems; (2) develop standards and guidelines for information systems used or operated by an agency or by a contractor on behalf of an agency, other than national security systems; and (3) develop standards and guidelines for providing adequate information security for all agency operations and assets.

Amends the Paperwork Reduction Act to require each agency to develop and maintain an inventory of major information systems (including major national security systems), including an identification of the interfaces between each such system and all other systems or networks.

Electronic Government Act of 2002

Sec. 1. SHORT TITLE; TABLE OF CONTENTS.

(a) Short Title.--This Act may be cited as the E-Government Act of 2002.

(b) Table of Contents.--The table of contents for this Act is as follows:

TITLE 40 - PUBLIC BUILDINGS, PROPERTY, AND WORKS

SUBTITLE III— Information Technology Management
CHAPTER 113—Responsibility for Acquisitions of Information Technology
SUBCHAPTER III – Other Responsibilities
Sec. 11331

TITLE 15 – COMMERCE AND TRADE-

CHAPTER 7 – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Sec 278g-3. Computer standards program
Sec 278g-4. Information Security and Privacy Advisory Board

TITLE 44 - CHAPTER 36 – Management and Promotion of Electronic Government Services

Sec. 3601. Definitions
Sec. 3602. Office of Electronic Government
Sec. 3603. Chief Information Officers Council
Sec. 3604. E-Government Fund
Sec. 3605. Program to encourage innovative solutions to enhance electronic Government services and processes
Sec. 3606. E-Government report
Sec. 3601. Definitions – Notes**:**

Findings and Purposes

Pub. L. 107–347, § 2, Dec. 17, 2002, 116 Stat. 2900, provided that:

(a) Findings.—Congress finds the following:

(1) The use of computers and the Internet is rapidly transforming societal interactions and the relationships among citizens, private businesses, and the Government.

(2) The Federal Government has had uneven success in applying advances in information technology to enhance governmental functions and

services, achieve more efficient performance, increase access to Government information, and increase citizen participation in Government.

(3) Most Internet-based services of the Federal Government are developed and presented separately, according to the jurisdictional boundaries of an individual department or agency, rather than being integrated cooperatively according to function or topic.

(4) Internet-based Government services involving interagency cooperation are especially difficult to develop and promote, in part because of a lack of sufficient funding mechanisms to support such interagency cooperation.

(5) Electronic Government has its impact through improved Government performance and outcomes within and across agencies.

(6) Electronic Government is a critical element in the management of Government, to be implemented as part of a management framework that also addresses finance, procurement, human capital, and other challenges to improve the performance of Government.

(7) To take full advantage of the improved Government performance that can be achieved through the use of Internet-based technology requires strong leadership, better organization, improved interagency collaboration, and more focused oversight of agency compliance with statutes related to information resource management.

(b) Purposes.—The purposes of this Act are the following:

(1) To provide effective leadership of Federal Government efforts to develop and promote electronic Government services and processes by establishing an Administrator of a new Office of Electronic Government within the Office of Management and Budget.

(2) To promote use of the Internet and other information technologies to provide increased opportunities for citizen participation in Government.

(3) To promote interagency collaboration in providing electronic Government services, where this collaboration would improve the service to citizens by integrating related functions, and in the use of

internal electronic Government processes, where this collaboration would improve the efficiency and effectiveness of the processes.

(4) To improve the ability of the Government to achieve agency missions and program performance goals.

(5) To promote the use of the Internet and emerging technologies within and across Government agencies to provide citizen-centric Government information and services.

(6) To reduce costs and burdens for businesses and other Government entities.

(7) To promote better informed decisionmaking by policy makers.

(8) To promote access to high quality Government information and services across multiple channels.

(9) To make the Federal Government more transparent and accountable.

(10) To transform agency operations by utilizing, where appropriate, best practices from public and private sector organizations.

(11) To provide enhanced access to Government information and services in a manner consistent with laws regarding protection of personal privacy, national security, records retention, access for persons with disabilities, and other relevant laws.

Sec. 3601. Definitions

In this chapter, the definitions under section 3502 shall apply, and the term—

(1) "Administrator" means the Administrator of the Office of Electronic Government established under section 3602;

(2) "Council" means the Chief Information Officers Council established under section 3603;

(3) "electronic Government" means the use by the Government of web-based Internet applications and other information technologies, combined with processes that implement these technologies, to—

(A) enhance the access to and delivery of Government information and services to the public, other agencies, and other Government entities; or

(B) bring about improvements in Government operations that may include effectiveness, efficiency, service quality, or transformation;

(4) "enterprise architecture"—

(A) means—

(i) a strategic information asset base, which defines the mission;

(ii) the information necessary to perform the mission;

(iii) the technologies necessary to perform the mission; and

(iv) the transitional processes for implementing new technologies in response to changing mission needs; and

(B) includes—

(i) a baseline architecture;

(ii) a target architecture; and

(iii) a sequencing plan;

(5) "Fund" means the E-Government Fund established under section 3604;

(6) "interoperability" means the ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner;

(7) "integrated service delivery" means the provision of Internet-based Federal Government information or services integrated according to function or topic rather than separated according to the boundaries of agency jurisdiction; and

(8) "tribal government" means—

(A) the governing body of any Indian tribe, band, nation, or other organized group or community located in the continental United States (excluding the State of Alaska) that is recognized as eligible for the special

programs and services provided by the United States to Indians because of their status as Indians, and

(B) any Alaska Native regional or village corporation established pursuant to the Alaska Native Claims Settlement Act (43 U.S.C. 1601 et seq.).

Sec. 3602. Office of Electronic Government

(a) There is established in the Office of Management and Budget an Office of Electronic Government.

(b) There shall be at the head of the Office an Administrator who shall be appointed by the President.

(c) The Administrator shall assist the Director in carrying out—

(1) all functions under this chapter;

(2) all of the functions assigned to the Director under title II of the E-Government Act of 2002; and

(3) other electronic government initiatives, consistent with other statutes.

(d) The Administrator shall assist the Director and the Deputy Director for Management and work with the Administrator of the Office of Information and Regulatory Affairs in setting strategic direction for implementing electronic Government, under relevant statutes, including—

(1) chapter 35;

(2) subtitle III of title 40, United States Code;

(3) section 552a of title 5 (commonly referred to as the "Privacy Act");

(4) the Government Paperwork Elimination Act (44 U.S.C. 3504 note); and

(5) the Federal Information Security Management Act of 2002.

(e) The Administrator shall work with the Administrator of the Office of Information and Regulatory Affairs and with other offices within the Office of Management and Budget to oversee implementation of electronic Government under this chapter, chapter 35, the E-

Government Act of 2002, and other relevant statutes, in a manner consistent with law, relating to—

(1) capital planning and investment control for information technology;

(2) the development of enterprise architectures;

(3) information security;

(4) privacy;

(5) access to, dissemination of, and preservation of Government information;

(6) accessibility of information technology for persons with disabilities; and

(7) other areas of electronic Government.

(f) Subject to requirements of this chapter, the Administrator shall assist the Director by performing electronic Government functions as follows:

(1) Advise the Director on the resources required to develop and effectively administer electronic Government initiatives.

(2) Recommend to the Director changes relating to Governmentwide strategies and priorities for electronic Government.

(3) Provide overall leadership and direction to the executive branch on electronic Government.

(4) Promote innovative uses of information technology by agencies, particularly initiatives involving multiagency collaboration, through support of pilot projects, research, experimentation, and the use of innovative technologies.

(5) Oversee the distribution of funds from, and ensure appropriate administration and coordination of, the E-Government Fund established under section 3604.

(6) Coordinate with the Administrator of General Services regarding programs undertaken by the General Services Administration to promote

electronic government and the efficient use of information technologies by agencies.

(7) Lead the activities of the Chief Information Officers Council established under section 3603 on behalf of the Deputy Director for Management, who shall chair the council.

(8) Assist the Director in establishing policies which shall set the framework for information technology standards for the Federal Government developed by the National Institute of Standards and Technology and promulgated by the Secretary of Commerce under section 11331 of title 40, taking into account, if appropriate, recommendations of the Chief Information Officers Council, experts, and interested parties from the private and nonprofit sectors and State, local, and tribal governments, and maximizing the use of commercial standards as appropriate, including the following:

(A) Standards and guidelines for interconnectivity and interoperability as described under section 3504.

(B) Consistent with the process under section 207(d) of the E-Government Act of 2002, standards and guidelines for categorizing Federal Government electronic information to enable efficient use of technologies, such as through the use of extensible markup language.

(C) Standards and guidelines for Federal Government computer system efficiency and security.

(9) Sponsor ongoing dialogue that—

(A) shall be conducted among Federal, State, local, and tribal government leaders on electronic Government in the executive, legislative, and judicial branches, as well as leaders in the private and nonprofit sectors, to encourage collaboration and enhance understanding of best practices and innovative approaches in acquiring, using, and managing information resources;

(B) is intended to improve the performance of governments in collaborating on the use of information technology to improve the delivery of Government information and services; and

(C) may include—

(i) development of innovative models—

(I) for electronic Government management and Government information technology contracts; and

(II) that may be developed through focused discussions or using separately sponsored research;

(ii) identification of opportunities for public-private collaboration in using Internet-based technology to increase the efficiency of Government-to-business transactions;

(iii) identification of mechanisms for providing incentives to program managers and other Government employees to develop and implement innovative uses of information technologies; and

(iv) identification of opportunities for public, private, and intergovernmental collaboration in addressing the disparities in access to the Internet and information technology.

(10) Sponsor activities to engage the general public in the development and implementation of policies and programs, particularly activities aimed at fulfilling the goal of using the most effective citizen-centered strategies and those activities which engage multiple agencies providing similar or related information and services.

(11) Oversee the work of the General Services Administration and other agencies in developing the integrated Internet-based system under section 204 of the E-Government Act of 2002.

(12) Coordinate with the Administrator for Federal Procurement Policy to ensure effective implementation of electronic procurement initiatives.

(13) Assist Federal agencies, including the General Services Administration, the Department of Justice, and the United States Access Board in—

(A) implementing accessibility standards under section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d); and

(B) ensuring compliance with those standards through the budget review process and other means.

(14) Oversee the development of enterprise architectures within and across agencies.

(15) Assist the Director and the Deputy Director for Management in overseeing agency efforts to ensure that electronic Government activities incorporate adequate, risk-based, and cost-effective security compatible with business processes.

(16) Administer the Office of Electronic Government established under this section.

(17) Assist the Director in preparing the E-Government report established under section 3606.

(g) The Director shall ensure that the Office of Management and Budget, including the Office of Electronic Government, the Office of Information and Regulatory Affairs, and other relevant offices, have adequate staff and resources to properly fulfill all functions under the E-Government Act of 2002.

Sec. 3603. Chief Information Officers Council

(a) There is established in the executive branch a Chief Information Officers Council.

(b) The members of the Council shall be as follows:

(1) The Deputy Director for Management of the Office of Management and Budget, who shall act as chairperson of the Council.

(2) The Administrator of the Office of Electronic Government.

(3) The Administrator of the Office of Information and Regulatory Affairs.

(4) The chief information officer of each agency described under section 901 (b) of title 31.

(5) The chief information officer of the Central Intelligence Agency.

(6) The chief information officer of the Department of the Army, the Department of the Navy, and the Department of the Air Force, if chief information officers have been designated for such departments under section 3506 (a)(2)(B).

(7) Any other officer or employee of the United States designated by the chairperson.

(c) (1) The Administrator of the Office of Electronic Government shall lead the activities of the Council on behalf of the Deputy Director for Management.

(2) (A) The Vice Chairman of the Council shall be selected by the Council from among its members.

(B) The Vice Chairman shall serve a 1-year term, and may serve multiple terms.

(3) The Administrator of General Services shall provide administrative and other support for the Council.

(d) The Council is designated the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of Federal Government information resources.

(e) In performing its duties, the Council shall consult regularly with representatives of State, local, and tribal governments.

(f) The Council shall perform functions that include the following:

(1) Develop recommendations for the Director on Government information resources management policies and requirements.

(2) Share experiences, ideas, best practices, and innovative approaches related to information resources management.

(3) Assist the Administrator in the identification, development, and coordination of multiagency projects and other innovative initiatives to improve Government performance through the use of information technology.

(4) Promote the development and use of common performance measures for agency information resources management under this chapter and title II of the E-Government Act of 2002.

(5) Work as appropriate with the National Institute of Standards and Technology and the Administrator to develop recommendations on information technology standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and promulgated under section 11331 of title 40, and maximize the use of commercial standards as appropriate, including the following:

(A) Standards and guidelines for interconnectivity and interoperability as described under section 3504.

(B) Consistent with the process under section 207(d) of the E-Government Act of 2002, standards and guideline for categorizing Federal Government electronic information to enable efficient use of technologies, such as through the use of extensible markup language.

(C) Standards and guidelines for Federal Government computer system efficiency and security.

(6) Work with the Office of Personnel Management to assess and address the hiring, training, classification, and professional development needs of the Government related to information resources management.

(7) Work with the Archivist of the United States to assess how the Federal Records Act can be addressed effectively by Federal information resources management activities.

Sec. 3604. E-Government Fund

(a)

(1) There is established in the Treasury of the United States the E-Government Fund.

(2) The Fund shall be administered by the Administrator of the General Services Administration to support projects approved by the Director, assisted by the Administrator of the Office of Electronic Government, that enable the Federal Government to expand its ability, through the development and

implementation of innovative uses of the Internet or other electronic methods, to conduct activities electronically.

(3) Projects under this subsection may include efforts to—

(A) make Federal Government information and services more readily available to members of the public (including individuals, businesses, grantees, and State and local governments);

(B) make it easier for the public to apply for benefits, receive services, pursue business opportunities, submit information, and otherwise conduct transactions with the Federal Government; and

(C) enable Federal agencies to take advantage of information technology in sharing information and conducting transactions with each other and with State and local governments.

(b)

(1) The Administrator shall—

(A) establish procedures for accepting and reviewing proposals for funding;

(B) consult with interagency councils, including the Chief Information Officers Council, the Chief Financial Officers Council, and other interagency management councils, in establishing procedures and reviewing proposals; and

(C) assist the Director in coordinating resources that agencies receive from the Fund with other resources available to agencies for similar purposes.

(2) When reviewing proposals and managing the Fund, the Administrator shall observe and incorporate the following procedures:

(A) A project requiring substantial involvement or funding from an agency shall be approved by a senior official with agencywide authority on behalf of the head of the agency, who shall report directly to the head of the agency.

(B) Projects shall adhere to fundamental capital planning and investment control processes.

(C) Agencies shall identify in their proposals resource commitments from the agencies involved and how these resources would be coordinated with support from the Fund, and include plans for potential continuation of projects after all funds made available from the Fund are expended.

(D) After considering the recommendations of the interagency councils, the Director, assisted by the Administrator, shall have final authority to determine which of the candidate projects shall be funded from the Fund.

(E) Agencies shall assess the results of funded projects.

(c) In determining which proposals to recommend for funding, the Administrator—

(1) shall consider criteria that include whether a proposal—

(A) identifies the group to be served, including citizens, businesses, the Federal Government, or other governments;

(B) indicates what service or information the project will provide that meets needs of groups identified under subparagraph (A);

(C) ensures proper security and protects privacy;

(D) is interagency in scope, including projects implemented by a primary or single agency that—

(i) could confer benefits on multiple agencies; and

(ii) have the support of other agencies; and

(E) has performance objectives that tie to agency missions and strategic goals, and interim results that relate to the objectives; and

(2) may also rank proposals based on criteria that include whether a proposal—

(A) has Governmentwide application or implications;

(B) has demonstrated support by the public to be served;

(C) integrates Federal with State, local, or tribal approaches to service delivery;

(D) identifies resource commitments from nongovernmental sectors;

(E) identifies resource commitments from the agencies involved;

(F) uses web-based technologies to achieve objectives;

(G) identifies records management and records access strategies;

(H) supports more effective citizen participation in and interaction with agency activities that further progress toward a more citizen-centered Government;

(I) directly delivers Government information and services to the public or provides the infrastructure for delivery;

(J) supports integrated service delivery;

(K) describes how business processes across agencies will reflect appropriate transformation simultaneous to technology implementation; and

(L) is new or innovative and does not supplant existing funding streams within agencies.

(d) The Fund may be used to fund the integrated Internet-based system under section 204 of the E-Government Act of 2002.

(e) None of the funds provided from the Fund may be transferred to any agency until 15 days after the Administrator of the General Services Administration has submitted to the Committees on Appropriations of the Senate and the House of Representatives, the Committee on Governmental Affairs of the Senate, the Committee on Government Reform of the House of Representatives, and the appropriate authorizing committees of the Senate and the House of Representatives, a notification and description of how the funds are to be allocated and how the expenditure will further the purposes of this chapter.

(f) (1) The Director shall report annually to Congress on the operation of the Fund, through the report established under section 3606.

(2) The report under paragraph (1) shall describe—

(A) all projects which the Director has approved for funding from the Fund; and

(B) the results that have been achieved to date for these funded projects.

(g) (1) There are authorized to be appropriated to the Fund—

(A) $45,000,000 for fiscal year 2003;

(B) $50,000,000 for fiscal year 2004;

(C) $100,000,000 for fiscal year 2005;

(D) $150,000,000 for fiscal year 2006; and

(E) such sums as are necessary for fiscal year 2007.

(2) Funds appropriated under this subsection shall remain available until expended.

Sec. 3605. Program to encourage innovative solutions to enhance electronic Government services and processes

(a) Establishment of Program.— The Administrator shall establish and promote a Governmentwide program to encourage contractor innovation and excellence in facilitating the development and enhancement of electronic Government services and processes.

(b) Issuance of Announcements Seeking Innovative Solutions.— Under the program, the Administrator, in consultation with the Council and the Administrator for Federal Procurement Policy, shall issue announcements seeking unique and innovative solutions to facilitate the development and enhancement of electronic Government services and processes.

(c) Multiagency Technical Assistance Team.—

(1) The Administrator, in consultation with the Council and the Administrator for Federal Procurement Policy, shall convene a multiagency technical assistance team to assist in screening proposals submitted to the Administrator to provide unique and innovative solutions to facilitate the development and enhancement of electronic Government services and processes. The team shall be composed of employees of the agencies represented on the Council who have expertise in scientific and technical disciplines that would facilitate the assessment of the feasibility of the proposals.

(2) The technical assistance team shall—

(A) assess the feasibility, scientific and technical merits, and estimated cost of each proposal; and

(B) submit each proposal, and the assessment of the proposal, to the Administrator.

(3) The technical assistance team shall not consider or evaluate proposals submitted in response to a solicitation for offers for a pending procurement or for a specific agency requirement.

(4) After receiving proposals and assessments from the technical assistance team, the Administrator shall consider recommending appropriate proposals for funding under the E-Government Fund established under section 3604 or, if appropriate, forward the proposal and the assessment of it to the executive agency whose mission most coincides with the subject matter of the proposal.

Sec. 3606. E-Government report

(a) Not later than March 1 of each year, the Director shall submit an E-Government status report to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives.

(b) The report under subsection (a) shall contain—

(1) a summary of the information reported by agencies under section 202(f) of the E-Government Act of 2002;

(2) the information required to be reported by section 3604 (f); and

(3) a description of compliance by the Federal Government with other goals and provisions of the E-Government Act of 2002.

TITLE 40 – SUBTITLE I – CHAPTER 3 – SUBCHAPTER I

Sec. 305. Electronic Government and information technologies

The Administrator of General Services shall consult with the Administrator of the Office of Electronic Government on programs undertaken by the General Services Administration to promote electronic Government and the efficient use of information technologies by Federal agencies.

TITLE 31 – SUBTITLE I – CHAPTER 5 – SUBCHAPTER I

Sec. 503. Functions of Deputy Director for Management

(b) Subject to the direction and approval of the Director, the Deputy Director for Management shall establish general management policies for executive agencies and perform the following general management functions:

(5) Chair the Chief Information Officers Council established under section 3603 of title 44.

Sec. 507. Office of Electronic Government

The Office of Electronic Government, established under section 3602 of title 44, is an office in the Office of Management and Budget.

TITLE 44 – CHAPTER 35 – SUBCHAPTER I – FEDERAL INFORMATION POLICY

Sec. 3501. Purposes – NOTES: Federal Management and Promotion of Electronic Government Services

Pub. L. 107–347, title II, Dec. 17, 2002, 116 Stat. 2910, provided that:

Sec. 201. Definitions

Except as otherwise provided, in this title the definitions under sections 3502 and 3601 of title 44, United States Code, shall apply.

Sec. 202. Federal Agency Responsibilities

(a) In General.—The head of each agency shall be responsible for—

(1) complying with the requirements of this Act [see Tables for classification] (including the amendments made by this Act), the related information resource management policies and guidance established by the Director of the Office of Management and Budget, and the related information technology standards promulgated by the Secretary of Commerce;

(2) ensuring that the information resource management policies and guidance established under this Act by the Director, and the related information technology standards promulgated by the Secretary of Commerce are communicated promptly and effectively to all relevant officials within their agency; and

(3) supporting the efforts of the Director and the Administrator of the General Services Administration to develop, maintain, and promote an integrated Internet-based system of delivering Federal Government information and services to the public under section 204.

(b) Performance Integration.—

(1) Agencies shall develop performance measures that demonstrate how electronic government enables progress toward agency objectives, strategic goals, and statutory mandates.

(2) In measuring performance under this section, agencies shall rely on existing data collections to the extent practicable.

(3) Areas of performance measurement that agencies should consider include—

(A) customer service;

(B) agency productivity; and

(C) adoption of innovative information technology, including the appropriate use of commercial best practices.

(4) Agencies shall link their performance goals, as appropriate, to key groups, including citizens, businesses, and other governments, and to internal Federal Government operations.

(5) As appropriate, agencies shall work collectively in linking their performance goals to groups identified under paragraph (4) and shall use information technology in delivering Government information and services to those groups.

(c) Avoiding Diminished Access.—When promulgating policies and implementing programs regarding the provision of Government information and services over the Internet, agency heads shall consider the impact on persons without access to the Internet, and shall, to the extent practicable—

(1) ensure that the availability of Government information and services has not been diminished for individuals who lack access to the Internet; and

(2) pursue alternate modes of delivery that make Government information and services more accessible to individuals who do not own computers or lack access to the Internet.

(d) Accessibility to People With Disabilities.—All actions taken by Federal departments and agencies under this Act [see Tables for classification] shall be in compliance with section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d).

(e) Sponsored Activities.—Agencies shall sponsor activities that use information technology to engage the public in the development and implementation of policies and programs.

(f) Chief Information Officers.—The Chief Information Officer of each of the agencies designated under chapter 36 of title 44, United States Code (as added by this Act) shall be responsible for—

(1) participating in the functions of the Chief Information Officers Council; and

(2) monitoring the implementation, within their respective agencies, of information technology standards promulgated by the Secretary of Commerce, including common standards for interconnectivity and interoperability, categorization of Federal Government electronic information, and computer system efficiency and security.

(g) E-Government Status Report.—

(1) In general.—Each agency shall compile and submit to the Director an annual E-Government Status Report on—

(A) the status of the implementation by the agency of electronic government initiatives;

(B) compliance by the agency with this Act [see Tables for classification]; and

(C) how electronic Government initiatives of the agency improve performance in delivering programs to constituencies.

(2) Submission.—Each agency shall submit an annual report under this subsection—

(A) to the Director at such time and in such manner as the Director requires;

(B) consistent with related reporting requirements; and

(C) which addresses any section in this title relevant to that agency.

(h) Use of Technology.—Nothing in this Act [see Tables for classification] supersedes the responsibility of an agency to use or manage information technology to deliver Government information and services that fulfill the statutory mission and programs of the agency.

(i) National Security Systems.—

(1) Inapplicability.—Except as provided under paragraph (2), this title does not apply to national security systems as defined in section 11103 of title 40, United States Code.

(2) Applicability.—This section, section 203, and section 214 do apply to national security systems to the extent practicable and consistent with law.

Sec. 203. Compatibility of Executive Agency Methods for Use and Acceptance of Electronic Signatures

(a) Purpose.—The purpose of this section is to achieve interoperable implementation of electronic signatures for appropriately secure electronic transactions with Government.

(b) Electronic Signatures.—In order to fulfill the objectives of the Government Paperwork Elimination Act (Public Law 105–277; 112 Stat. 2681–749 through 2681–751) [44 U.S.C. 3504 note], each Executive agency (as defined under section 105 of title 5, United States Code) shall ensure that its methods for use and acceptance of electronic signatures are compatible with the relevant policies and procedures issued by the Director.

(c) Authority for Electronic Signatures.—The Administrator of General Services shall support the Director by establishing a framework to allow efficient interoperability among Executive agencies when using electronic signatures, including processing of digital signatures.

(d) Authorization of Appropriations.—There are authorized to be appropriated to the General Services Administration, to ensure the development and operation of a Federal bridge certification authority for digital signature compatibility, and for other activities consistent with this section, $8,000,000 or such sums as are necessary in fiscal year 2003, and such sums as are necessary for each fiscal year thereafter.

Sec. 204. Federal Internet Portal

(a) In General.—

(1) Public access.—The Director shall work with the Administrator of the General Services Administration and other agencies to maintain and promote an integrated Internet-based system of providing the public with access to Government information and services.

(2) Criteria.—To the extent practicable, the integrated system shall be designed and operated according to the following criteria:

(A) The provision of Internet-based Government information and services directed to key groups, including citizens, business, and other governments, and integrated according to function or topic rather than separated according to the boundaries of agency jurisdiction.

(B) An ongoing effort to ensure that Internet-based Government services relevant to a given citizen activity are available from a single point.

(C) Access to Federal Government information and services consolidated, as appropriate, with Internet-based information and services provided by State, local, and tribal governments.

(D) Access to Federal Government information held by 1 or more agencies shall be made available in a manner that protects privacy, consistent with law.

(b) Authorization of Appropriations.—There are authorized to be appropriated to the General Services Administration $15,000,000 for the maintenance, improvement, and promotion of the integrated Internet-based system for fiscal year 2003, and such sums as are necessary for fiscal years 2004 through 2007.

Sec. 207. Accessibility, Usability, and Preservation of Government Information

(a) Purpose.—The purpose of this section is to improve the methods by which Government information, including information on the Internet, is organized, preserved, and made accessible to the public.

(b) Definitions.—In this section, the term—

(1) 'Committee' means the Interagency Committee on Government Information established under subsection (c); and

(2) 'directory' means a taxonomy of subjects linked to websites that—

(A) organizes Government information on the Internet according to subject matter; and

(B) may be created with the participation of human editors.

(c) Interagency Committee.—

(1) Establishment.—Not later than 180 days after the date of enactment of this title [Dec. 17, 2002], the Director shall establish the Interagency Committee on Government Information.

(2) Membership.—The Committee shall be chaired by the Director or the designee of the Director and— (A) shall include representatives from—

(i) the National Archives and Records Administration;

(ii) the offices of the Chief Information Officers from Federal agencies; and

(iii) other relevant officers from the executive branch; and

(B) may include representatives from the Federal legislative and judicial branches.

(3) Functions.—The Committee shall—

(A) engage in public consultation to the maximum extent feasible, including consultation with interested communities such as public advocacy organizations;

(B) conduct studies and submit recommendations, as provided under this section, to the Director and Congress; and

(C) share effective practices for access to, dissemination of, and retention of Federal information.

(4) Termination.—The Committee may be terminated on a date determined by the Director, except the Committee may not terminate before the Committee submits all recommendations required under this section.

(d) Categorizing of Information.—

(1) Committee functions.—Not later than 2 years after the date of enactment of this Act [Dec. 17, 2002], the Committee shall submit recommendations to the Director on—

(A) the adoption of standards, which are open to the maximum extent feasible, to enable the organization and categorization of Government information—

(i) in a way that is searchable electronically, including by searchable identifiers; and

(ii) in ways that are interoperable across agencies;

(B) the definition of categories of Government information which should be classified under the standards; and

(C) determining priorities and developing schedules for the initial implementation of the standards by agencies.

(2) Functions of the director.—Not later than 1 year after the submission of recommendations under paragraph (1), the Director shall issue policies—

(A) requiring that agencies use standards, which are open to the maximum extent feasible, to enable the organization and categorization of Government information—

(i) in a way that is searchable electronically, including by searchable identifiers;

(ii) in ways that are interoperable across agencies; and

(iii) that are, as appropriate, consistent with the provisions under section 3602 (f)(8) of title 44, United States Code;

(B) defining categories of Government information which shall be required to be classified under the standards; and

(C) determining priorities and developing schedules for the initial implementation of the standards by agencies.

(3) Modification of policies.—After the submission of agency reports under paragraph (4), the Director shall modify the policies, as needed, in consultation with the Committee and interested parties.

(4) Agency functions.—Each agency shall report annually to the Director, in the report established under section 202 (g), on compliance of that agency with the policies issued under paragraph (2)(A).

(e) Public Access to Electronic Information.—

(1) Committee functions.—Not later than 2 years after the date of enactment of this Act [Dec. 17, 2002], the Committee shall submit recommendations to the Director and the Archivist of the United States on—

(A) the adoption by agencies of policies and procedures to ensure that chapters 21, 25, 27, 29, and 31 of title 44, United States Code, are applied effectively and comprehensively to Government information on the Internet and to other electronic records; and

(B) the imposition of timetables for the implementation of the policies and procedures by agencies.

(2) Functions of the archivist.—Not later than 1 year after the submission of recommendations by the Committee under paragraph (1), the Archivist of the United States shall issue policies—

(A) requiring the adoption by agencies of policies and procedures to ensure that chapters 21, 25, 27, 29, and 31 of title 44, United States

Code, are applied effectively and comprehensively to Government information on the Internet and to other electronic records; and

(B) imposing timetables for the implementation of the policies, procedures, and technologies by agencies.

(3) Modification of policies.—After the submission of agency reports under paragraph (4), the Archivist of the United States shall modify the policies, as needed, in consultation with the Committee and interested parties.

(4) Agency functions.—Each agency shall report annually to the Director, in the report established under section 202 (g), on compliance of that agency with the policies issued under paragraph (2)(A).

(f) Agency Websites.—

(1) Standards for agency websites.—Not later than 2 years after the effective date of this title [see Effective Date note set out under section 3601 of this title], the Director shall promulgate guidance for agency websites that includes—

(A) requirements that websites include direct links to—

(i) descriptions of the mission and statutory authority of the agency;

(ii) information made available to the public under subsections (a)(1) and (b) of section 552 of title 5, United States Code (commonly referred to as the 'Freedom of Information Act');

(iii) information about the organizational structure of the agency; and

(iv) the strategic plan of the agency developed under section 306 of title 5, United States Code; and

(B) minimum agency goals to assist public users to navigate agency websites, including—

(i) speed of retrieval of search results;

(ii) the relevance of the results;

(iii) tools to aggregate and disaggregate data; and

(iv) security protocols to protect information.

(2) Agency requirements.—

(A) Not later than 2 years after the date of enactment of this Act [Dec. 17, 2002], each agency shall—

(i) consult with the Committee and solicit public comment;

(ii) establish a process for determining which Government information the agency intends to make available and accessible to the public on the Internet and by other means;

(iii) develop priorities and schedules for making Government information available and accessible;

(iv) make such final determinations, priorities, and schedules available for public comment;

(v) post such final determinations, priorities, and schedules on the Internet; and

(vi) submit such final determinations, priorities, and schedules to the Director, in the report established under section 202 (g).

(B) Each agency shall update determinations, priorities, and schedules of the agency, as needed, after consulting with the Committee and soliciting public comment, if appropriate.

(3) Public domain directory of public federal government websites.—

(A) Establishment.—Not later than 2 years after the effective date of this title [see Effective Date note set out under section 3601 of this title], the Director and each agency shall—

(i) develop and establish a public domain directory of public Federal Government websites; and

(ii) post the directory on the Internet with a link to the integrated Internet-based system established under section 204.

(B) Development.—With the assistance of each agency, the Director shall—

(i) direct the development of the directory through a collaborative effort, including input from—

(I) agency librarians;

(II) information technology managers;

(III) program managers;

(IV) records managers;

(V) Federal depository librarians; and

(VI) other interested parties; and

(ii) develop a public domain taxonomy of subjects used to review and categorize public Federal Government websites.

(C) Update.—With the assistance of each agency, the Administrator of the Office of Electronic Government shall—

(i) update the directory as necessary, but not less than every 6 months; and

(ii) solicit interested persons for improvements to the directory.

(g) Access to Federally Funded Research and Development.—

(1) Development and maintenance of governmentwide repository and website.—

(A) Repository and website.—The Director of the Office of Management and Budget (or the Director's delegate), in consultation with the Director of the Office of Science and Technology Policy and other relevant agencies, shall ensure the development and maintenance of—

(i) a repository that fully integrates, to the maximum extent feasible, information about research and development funded by the Federal Government, and the repository shall—

(I) include information about research and development funded by the Federal Government, consistent with any relevant protections for the information under section 552 of title 5, United States Code, and performed by— "(aa) institutions not a part of the Federal Government,

including State, local, and foreign governments; industrial firms; educational institutions; not-for-profit organizations; federally funded research and development centers; and private individuals; and “(bb) entities of the Federal Government, including research and development laboratories, centers, and offices; and

(II) integrate information about each separate research and development task or award, including—

(aa) the dates upon which the task or award is expected to start and end;

(bb) a brief summary describing the objective and the scientific and technical focus of the task or award;

(cc) the entity or institution performing the task or award and its contact information;

(dd) the total amount of Federal funds expected to be provided to the task or award over its lifetime and the amount of funds expected to be provided in each fiscal year in which the work of the task or award is ongoing;

(ee) any restrictions attached to the task or award that would prevent the sharing with the general public of any or all of the information required by this subsection, and the reasons for such restrictions; and

(ff) such other information as may be determined to be appropriate; and

(ii) 1 or more websites upon which all or part of the repository of Federal research and development shall be made available to and searchable by Federal agencies and non-Federal entities, including the general public, to facilitate—

(I) the coordination of Federal research and development activities;

(II) collaboration among those conducting Federal research and development;

(III) the transfer of technology among Federal agencies and between Federal agencies and non-Federal entities; and (IV) access

by policymakers and the public to information concerning Federal research and development activities.

(B) Oversight.—The Director of the Office of Management and Budget shall issue any guidance determined necessary to ensure that agencies provide all information requested under this subsection.

(2) Agency functions.—Any agency that funds Federal research and development under this subsection shall provide the information required to populate the repository in the manner prescribed by the Director of the Office of Management and Budget.

(3) Committee functions.—Not later than 18 months after the date of enactment of this Act [Dec. 17, 2002], working with the Director of the Office of Science and Technology Policy, and after consultation with interested parties, the Committee shall submit recommendations to the Director on—

(A) policies to improve agency reporting of information for the repository established under this subsection; and

(B) policies to improve dissemination of the results of research performed by Federal agencies and federally funded research and development centers.

(4) Functions of the director.—After submission of recommendations by the Committee under paragraph (3), the Director shall report on the recommendations of the Committee and Director to Congress, in the E-Government report under section 3606 of title 44 (as added by this Act).

(5) Authorization of appropriations.—There are authorized to be appropriated for the development, maintenance, and operation of the Governmentwide repository and website under this subsection—

(A) $2,000,000 in each of the fiscal years 2003 through 2005; and

(B) such sums as are necessary in each of the fiscal years 2006 and 2007.

Sec. 208. Privacy Provisions

(a) Purpose.—The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

(b) Privacy Impact Assessments.—

(1) Responsibilities of agencies.—

(A) In general.—An agency shall take actions described under subparagraph (B) before—

(i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or

(ii) initiating a new collection of information that—

(I) will be collected, maintained, or disseminated using information technology; and

(II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

(B) Agency activities.—To the extent required under subparagraph (A), each agency shall—

(i) conduct a privacy impact assessment;

(ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and

(iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

(C) Sensitive information.—Subparagraph (B)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.

(D) Copy to director.—Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.

(2) Contents of a privacy impact assessment.—

(A) In general.—The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.

(B) Guidance.—The guidance shall—

(i) ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and

(ii) require that a privacy impact assessment address—

(I) what information is to be collected;

(II) why the information is being collected;

(III) the intended use of the agency of the information;

(IV) with whom the information will be shared;

(V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;

(VI) how the information will be secured; and

(VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the 'Privacy Act').

(3) Responsibilities of the director.—The Director shall—

(A) develop policies and guidelines for agencies on the conduct of privacy impact assessments;

(B) oversee the implementation of the privacy impact assessment process throughout the Government; and

(C) require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

(c) Privacy Protections on Agency Websites.—

(1) Privacy policies on websites.—

(A) Guidelines for notices.—The Director shall develop guidance for privacy notices on agency websites used by the public.

(B) Contents.—The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—

(i) what information is to be collected;

(ii) why the information is being collected;

(iii) the intended use of the agency of the information;

(iv) with whom the information will be shared;

(v) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;

(vi) how the information will be secured; and

(vii) the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the 'Privacy Act'), and other laws relevant to the protection of the privacy of an individual.

(2) Privacy policies in machine-readable formats.—The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

(d) Definition.—In this section, the term 'identifiable form' means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Sec. 209. Federal Information Technology Workforce Development

(a) Purpose.—The purpose of this section is to improve the skills of the Federal workforce in using information technology to deliver Government information and services.

(b) Workforce Development.—

(1) In general.—In consultation with the Director of the Office of Management and Budget, the Chief Information Officers Council, and

the Administrator of General Services, the Director of the Office of Personnel Management shall—

(A) analyze, on an ongoing basis, the personnel needs of the Federal Government related to information technology and information resource management;

(B) identify where current information technology and information resource management training do not satisfy the personnel needs described in subparagraph (A);

(C) oversee the development of curricula, training methods, and training priorities that correspond to the projected personnel needs of the Federal Government related to information technology and information resource management; and

(D) assess the training of Federal employees in information technology disciplines in order to ensure that the information resource management needs of the Federal Government are addressed.

(2) Information technology training programs.—The head of each Executive agency, after consultation with the Director of the Office of Personnel Management, the Chief Information Officers Council, and the Administrator of General Services, shall establish and operate information technology training programs consistent with the requirements of this subsection. Such programs shall—

(A) have curricula covering a broad range of information technology disciplines corresponding to the specific information technology and information resource management needs of the agency involved;

(B) be developed and applied according to rigorous standards; and

(C) be designed to maximize efficiency, through the use of self-paced courses, online courses, on-the-job training, and the use of remote instructors, wherever such features can be applied without reducing the effectiveness of the training or negatively impacting academic standards.

(3) Governmentwide policies and evaluation.—The Director of the Office of Personnel Management, in coordination with the Director of the Office of Management and Budget, shall issue policies to promote the

development of performance standards for training and uniform implementation of this subsection by Executive agencies, with due regard for differences in program requirements among agencies that may be appropriate and warranted in view of the agency mission. The Director of the Office of Personnel Management shall evaluate the implementation of the provisions of this subsection by Executive agencies.

(4) Chief information officer authorities and responsibilities.—Subject to the authority, direction, and control of the head of an Executive agency, the chief information officer of such agency shall carry out all powers, functions, and duties of the head of the agency with respect to implementation of this subsection. The chief information officer shall ensure that the policies of the agency head established in accordance with this subsection are implemented throughout the agency.

(5) Information technology training reporting.—The Director of the Office of Management and Budget shall ensure that the heads of Executive agencies collect and maintain standardized information on the information technology and information resources management workforce related to the implementation of this subsection.

(6) Authority to detail employees to non-Federal employers.—In carrying out the preceding provisions of this subsection, the Director of the Office of Personnel Management may provide for a program under which a Federal employee may be detailed to a non-Federal employer. The Director of the Office of Personnel Management shall prescribe regulations for such program, including the conditions for service and duties as the Director considers necessary.

(7) Coordination provision.—An assignment described in section 3703 of title 5, United States Code, may not be made unless a program under paragraph (6) is established, and the assignment is made in accordance with the requirements of such program.

(8) Employee participation.—Subject to information resource management needs and the limitations imposed by resource needs in other occupational areas, and consistent with their overall workforce development strategies, agencies shall encourage employees to participate in occupational information technology training.

(9) Authorization of Appropriations.—There are authorized to be appropriated to the Office of Personnel Management for the implementation of this subsection, $15,000,000 in fiscal year 2003, and such sums as are necessary for each fiscal year thereafter.

(10) Executive agency defined.—For purposes of this subsection, the term ‘Executive agency’ has the meaning given the term ‘agency’ under section 3701 of title 5, United States Code (as added by subsection (c)).

(c) Information Technology Exchange Program.—

(1) In general.—[Enacted chapter 37 of Title 5, Government

Organization and Employees.]

(2) Report.—Not later than 4 years after the date of the enactment of this Act [Dec. 17, 2002], the General Accounting Office shall prepare and submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate a report on the operation of chapter 37 of title 5, United States Code (as added by this subsection). Such report shall include—

(A) an evaluation of the effectiveness of the program established by such chapter; and

(B) a recommendation as to whether such program should be continued (with or without modification) or allowed to lapse.

(3) Clerical Amendment.—[Amended analysis for part III of Title 5.]

(d) Ethics Provisions.—

(1) One-year restriction on certain communications.—[Amended section 207 of Title 18, Crimes and Criminal Procedure.]

(2) Disclosure of confidential information.—[Amended section 1905 of Title 18.]

(3) Contract advice.—[Amended section 207 of Title 18.]

(4) Restriction on disclosure of procurement information. [Amended section 423 of Title 41, Public Contracts.]

(e) Report on Existing Exchange Programs.—

(1) Exchange program defined.—For purposes of this subsection, the term ‘exchange program’ means an executive exchange program, the program under subchapter VI of chapter 33 of title 5, United States Code, and any other program which allows for—

(A) the assignment of employees of the Federal Government to non-Federal employers;

(B) the assignment of employees of non-Federal employers to the Federal Government; or

(C) both.

(2) Reporting requirement.—Not later than 1 year after the date of the enactment of this Act [Dec. 17, 2002], the Office of Personnel Management shall prepare and submit to the Committee on Government Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate a report identifying all existing exchange programs.

(3) Specific information.—The report shall, for each such program, include—

(A) a brief description of the program, including its size, eligibility requirements, and terms or conditions for participation;

(B) specific citation to the law or other authority under which the program is established;

(C) the names of persons to contact for more information, and how they may be reached; and

(D) any other information which the Office considers appropriate.

(f) Report on the Establishment of a Governmentwide Information Technology Training Program.—

(1) In general.—Not later January 1, 2003, the Office of Personnel Management, in consultation with the Chief Information Officers Council and the Administrator of General Services, shall review and submit to the Committee on Government Reform of the House of

Representatives and the Committee on Governmental Affairs of the Senate a written report on the following:

(A) The adequacy of any existing information technology training programs available to Federal employees on a Governmentwide basis.

(B)(i) If one or more such programs already exist, recommendations as to how they might be improved.

(ii) If no such program yet exists, recommendations as to how such a program might be designed and established.

(C) With respect to any recommendations under subparagraph (B), how the program under chapter 37 of title 5, United States Code, might be used to help carry them out.

(2) Cost estimate.—The report shall, for any recommended program (or improvements) under paragraph (1)(B), include the estimated costs associated with the implementation and operation of such program as so established (or estimated difference in costs of any such program as so improved).

(g) Technical and Conforming Amendments.—

(1) Amendments to title 5, united states code.—[Amended sections 3111, 4108, and 7353 of Title 5.]

(2) Amendment to title 18, united states code.—[Amended section 209 of Title 18.]

(3) Other amendments.—[Amended section 125(c)(1) of Pub. L. 100–238, set out as a note under section 8432 of Title 5.]

Sec. 210. Share-In-Savings Initiatives

(a) Defense Contracts.—[Enacted section 2332 of Title 10, Armed Forces.]

(b) Other Contracts.—[Enacted section 266a of Title 41.]

(c) Development of Incentives.—The Director of the Office of Management and Budget shall, in consultation with the Committee on Governmental Affairs of the Senate, the Committee on Government Reform of the House of Representatives, and executive agencies,

develop techniques to permit an executive agency to retain a portion of the savings (after payment of the contractor's share of the savings) derived from share-in-savings contracts as funds are appropriated to the agency in future fiscal years.

(d) Regulations.—Not later than 270 days after the date of the enactment of this Act [Dec. 17, 2002], the Federal Acquisition Regulation shall be revised to implement the provisions enacted by this section. Such revisions shall—

(1) provide for the use of competitive procedures in the selection and award of share-in-savings contracts to—

(A) ensure the contractor's share of savings reflects the risk involved and market conditions; and

(B) otherwise yield greatest value to the government; and

(2) allow appropriate regulatory flexibility to facilitate the use of share-in-savings contracts by executive agencies, including the use of innovative provisions for technology refreshment and nonstandard Federal Acquisition Regulation contract clauses.

(e) Additional Guidance.—The Administrator of General Services shall—

(1) identify potential opportunities for the use of share-in-savings contracts; and

(2) in consultation with the Director of the Office of Management and Budget, provide guidance to executive agencies for determining mutually beneficial savings share ratios and baselines from which savings may be measured.

(f) OMB Report to Congress.—In consultation with executive agencies, the Director of the Office of Management and Budget shall, not later than 2 years after the date of the enactment of this Act [Dec. 17, 2002], submit to Congress a report containing—

(1) a description of the number of share-in-savings contracts entered into by each executive agency under by [sic] this section and the amendments made by this section, and, for each contract identified—

(A) the information technology acquired;

(B) the total amount of payments made to the contractor; and

(C) the total amount of savings or other measurable benefits realized;

(2) a description of the ability of agencies to determine the baseline costs of a project against which savings can be measured; and

(3) any recommendations, as the Director deems appropriate, regarding additional changes in law that may be necessary to ensure effective use of share-in-savings contracts by executive agencies.

(g) GAO Report to Congress.—The Comptroller General shall, not later than 6 months after the report required under subsection

(f) is submitted to Congress, conduct a review of that report and submit to Congress a report containing—

(1) the results of the review;

(2) an independent assessment by the Comptroller General of the effectiveness of the use of share-in-savings contracts in improving the mission-related and administrative processes of the executive agencies and the achievement of agency missions; and

(3) a recommendation on whether the authority to enter into share-in-savings contracts should be continued.

(h) Repeal of Share-in-Savings Pilot Program.—

(1) Repeal.—[Repealed section 11521 of Title 40, Public Buildings, Property, and Works.]

(2) Conforming amendments to pilot program authority.—[Amended sections 11501 to 11505 of Title 40.]

(3) Additional conforming amendments.—[Redesignated 11522 of Title 40 as 11521 and amended headings and analysis.]

(i) Definitions.—In this section, the terms ‘contractor’, ‘savings’, and ‘share-in-savings contract’ have the meanings given those terms in

section 317 of the Federal Property and Administrative Services Act of 1949 [41 U.S.C. 266a] (as added by subsection (b)).

Sec. 212. Integrated Reporting Study and Pilot Projects

(a) Purposes.—The purposes of this section are to—

(1) enhance the interoperability of Federal information systems;

(2) assist the public, including the regulated community, in electronically submitting information to agencies under Federal requirements, by reducing the burden of duplicate collection and ensuring the accuracy of submitted information; and

(3) enable any person to integrate and obtain similar information held by 1 or more agencies under 1 or more Federal requirements without violating the privacy rights of an individual.

(b) Definitions.—In this section, the term—

(1) 'agency' means an Executive agency as defined under section 105 of title 5, United States Code; and

(2) 'person' means any individual, trust, firm, joint stock company, corporation (including a government corporation), partnership, association, State, municipality, commission, political subdivision of a State, interstate body, or agency or component of the Federal Government.

(c) Report.—

(1) In general.—Not later than 3 years after the date of enactment of this Act [Dec. 17, 2002], the Director shall oversee a study, in consultation with agencies, the regulated community, public interest organizations, and the public, and submit a report to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives on progress toward integrating Federal information systems across agencies.

(2) Contents.—The report under this section shall—

(A) address the integration of data elements used in the electronic collection of information within databases established under Federal

statute without reducing the quality, accessibility, scope, or utility of the information contained in each database;

(B) address the feasibility of developing, or enabling the development of, software, including Internet-based tools, for use by reporting persons in assembling, documenting, and validating the accuracy of information electronically submitted to agencies under nonvoluntary, statutory, and regulatory requirements;

(C) address the feasibility of developing a distributed information system involving, on a voluntary basis, at least 2 agencies, that—

(i) provides consistent, dependable, and timely public access to the information holdings of 1 or more agencies, or some portion of such holdings, without requiring public users to know which agency holds the information; and

(ii) allows the integration of public information held by the participating agencies;

(D) address the feasibility of incorporating other elements related to the purposes of this section at the discretion of the Director; and

(E) make any recommendations that the Director deems appropriate on the use of integrated reporting and information systems, to reduce the burden on reporting and strengthen public access to databases within and across agencies.

(d) Pilot Projects To Encourage Integrated Collection and Management of Data and Interoperability of Federal Information Systems.—

(1) In general.—In order to provide input to the study under subsection (c), the Director shall designate, in consultation with agencies, a series of no more than 5 pilot projects that integrate data elements. The Director shall consult with agencies, the regulated community, public interest organizations, and the public on the implementation of the pilot projects.

(2) Goals of pilot projects.—

(A) In general.—Each goal described under subparagraph (B) shall be addressed by at least 1 pilot project each.

(B) Goals.—The goals under this paragraph are to—

(i) reduce information collection burdens by eliminating duplicative data elements within 2 or more reporting requirements;

(ii) create interoperability between or among public databases managed by 2 or more agencies using technologies and techniques that facilitate public access; and

(iii) develop, or enable the development of, software to reduce errors in electronically submitted information.

(3) Input.—Each pilot project shall seek input from users on the utility of the pilot project and areas for improvement. To the extent practicable, the Director shall consult with relevant agencies and State, tribal, and local governments in carrying out the report and pilot projects under this section.

(e) Protections.—The activities authorized under this section shall afford protections for—

(1) confidential business information consistent with section 552 (b)(4) of title 5, United States Code, and other relevant law;

(2) personal privacy information under sections 552 (b)(6) and (7)(C) and 552a of title 5, United States Code, and other relevant law;

(3) other information consistent with section 552 (b)(3) of title 5, United States Code, and other relevant law; and

(4) confidential statistical information collected under a confidentiality pledge, solely for statistical purposes, consistent with the Office of Management and Budget's Federal Statistical Confidentiality Order, and other relevant law.

Sec. 214. Enhancing Crisis Management Through Advanced Information Technology

(a) Purpose.—The purpose of this section is to improve how information technology is used in coordinating and facilitating information on disaster preparedness, response, and recovery, while ensuring the availability of such information across multiple access channels.

(b) In General.—

(1) Study on enhancement of crisis response.—Not later than 90 days after the date of enactment of this Act [Dec. 17, 2002], the Administrator, in consultation with the Federal Emergency Management Agency, shall ensure that a study is conducted on using information technology to enhance crisis preparedness, response, and consequence management of natural and manmade disasters.

(2) Contents.—The study under this subsection shall address—

(A) a research and implementation strategy for effective use of information technology in crisis response and consequence management, including the more effective use of technologies, management of information technology research initiatives, and incorporation of research advances into the information and communications systems of—

(i) the Federal Emergency Management Agency; and

(ii) other Federal, State, and local agencies responsible for crisis preparedness, response, and consequence management; and

(B) opportunities for research and development on enhanced technologies into areas of potential improvement as determined during the course of the study.

(3) Report.—Not later than 2 years after the date on which a contract is entered into under paragraph (1), the Administrator shall submit a report on the study, including findings and recommendations to—

(A) the Committee on Governmental Affairs of the Senate; and

(B) the Committee on Government Reform of the House of Representatives.

(4) Interagency cooperation.—Other Federal departments and agencies with responsibility for disaster relief and emergency assistance shall fully cooperate with the Administrator in carrying out this section.

(5) Authorization of appropriations.—There are authorized to be appropriated for research under this subsection, such sums as are necessary for fiscal year 2003.

(c) Pilot Projects.—Based on the results of the research conducted under subsection (b), the Administrator, in consultation with the Federal Emergency Management Agency, shall initiate pilot projects or report to Congress on other activities that further the goal of maximizing the utility of information technology in disaster management. The Administrator shall cooperate with other relevant agencies, and, if appropriate, State, local, and tribal governments, in initiating such pilot projects.

Sec. 216. Common Protocols for Geographic Information Systems

(a) Purposes.—The purposes of this section are to—

(1) reduce redundant data collection and information; and

(2) promote collaboration and use of standards for government geographic information.

(b) Definition.—In this section, the term ‘geographic information’ means information systems that involve locational data, such as maps or other geospatial information resources.

(c) In General.—

(1) Common protocols.—The Administrator, in consultation with the Secretary of the Interior, working with the Director and through an interagency group, and working with private sector experts, State, local, and tribal governments, commercial and international standards groups, and other interested parties, shall facilitate the development of common protocols for the development, acquisition, maintenance, distribution,

and application of geographic information. If practicable, the Administrator shall incorporate intergovernmental and public private geographic information partnerships into efforts under this subsection.

(2) Interagency group.—The interagency group referred to under paragraph (1) shall include representatives of the National Institute of Standards and Technology and other agencies.

(d) Director.—The Director shall oversee—

(1) the interagency initiative to develop common protocols;

(2) the coordination with State, local, and tribal governments, public private partnerships, and other interested persons on effective and efficient ways to align geographic information and develop common protocols; and

(3) the adoption of common standards relating to the protocols.

(e) Common Protocols.—The common protocols shall be designed to—

(1) maximize the degree to which unclassified geographic information from various sources can be made electronically compatible and accessible; and

(2) promote the development of interoperable geographic information systems technologies that shall—

(A) allow widespread, low-cost use and sharing of geographic data by Federal agencies, State, local, and tribal governments, and the public; and

(B) enable the enhancement of services using geographic data.

(f) Authorization of Appropriations.—There are authorized to be appropriated such sums as are necessary to carry out this section, for each of the fiscal years 2003 through 2007."

TITLE 44 – CHAPTER 35 – SUBCHAPTER I – FEDERAL INFORMATION POLICY

Sec. 3505. Assignment of tasks and deadlines

(a) In carrying out the functions under this subchapter, the Director shall—

(1) in consultation with agency heads, set an annual Governmentwide goal for the reduction of information collection burdens by at least 10 percent during each of fiscal years 1996 and 1997 and 5 percent during each of fiscal years 1998, 1999, 2000, and 2001, and set annual agency goals to—

(A) reduce information collection burdens imposed on the public that—

(i) represent the maximum practicable opportunity in each agency; and

(ii) are consistent with improving agency management of the process for the review of collections of information established under section 3506 (c); and

(B) improve information resources management in ways that increase the productivity, efficiency and effectiveness of Federal programs, including service delivery to the public;

(2) with selected agencies and non-Federal entities on a voluntary basis, conduct pilot projects to test alternative policies, practices, regulations, and procedures to fulfill the purposes of this subchapter, particularly with regard to minimizing the Federal information collection burden; and

(3) in consultation with the Administrator of General Services, the Director of the National Institute of Standards and Technology, the Archivist of the United States, and the Director of the Office of Personnel Management, develop and maintain a Governmentwide strategic plan for information resources management, that shall include—

(A) a description of the objectives and the means by which the Federal Government shall apply information resources to improve agency and program performance;

(B) plans for—

(i) reducing information burdens on the public, including reducing such burdens through the elimination of duplication and meeting shared data needs with shared resources;

(ii) enhancing public access to and dissemination of, information, using electronic and other formats; and

(iii) meeting the information technology needs of the Federal Government in accordance with the purposes of this subchapter; and

(C) a description of progress in applying information resources management to improve agency performance and the accomplishment of missions.

(b) For purposes of any pilot project conducted under subsection (a)(2), the Director may, after consultation with the agency head, waive the application of any administrative directive issued by an agency with which the project is conducted, including any directive requiring a collection of information, after giving timely notice to the public and the Congress regarding the need for such waiver.

(c) Inventory of Major Information Systems.—(1) The head of each agency shall develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of such agency.

(2) The identification of information systems in an inventory under this subsection shall include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.

(3) Such inventory shall be—

(A) updated at least annually;

(B) made available to the Comptroller General; and

(C) used to support information resources management, including—

(i) preparation and maintenance of the inventory of information resources under section 3506 (b)(4);

(ii) information technology planning, budgeting, acquisition, and management under section 3506 (h), subtitle III of title 40, and related laws and guidance;

(iii) monitoring, testing, and evaluation of information security controls under subchapter II; (iv) preparation of the index of major information systems required under section 552 (g) of title 5, United States Code; and

(v) preparation of information system inventories required for records management under chapters 21, 29, 31, and 33.

(4) The Director shall issue guidance for and oversee the implementation of the requirements of this subsection.

TITLE 5 – PART III – Subpart B – CHAPTER 37 – INFORMATION TECHNOLOGY EXCHANGE PROGRAM

Sec. 3701. Definitions

For purposes of this chapter—

(1) the term “agency” means an Executive agency, but does not include the General Accounting Office; and

(2) the term “detail” means—

(A) the assignment or loan of an employee of an agency to a private sector organization without a change of position from the agency that employs the individual, or

(B) the assignment or loan of an employee of a private sector organization to an agency without a change of position from the private sector organization that employs the individual, whichever is appropriate in the context in which such term is used.

Sec. 3702. General provisions

(a) Assignment Authority**.—** On request from or with the agreement of a private sector organization, and with the consent of the employee concerned, the head of an agency may arrange for the assignment of an employee of the agency to a private sector organization or an employee of a private sector organization to the agency. An eligible employee is an individual who—

(1) works in the field of information technology management;

(2) is considered an exceptional performer by the individual's current employer; and

(3) is expected to assume increased information technology management responsibilities in the future.

An employee of an agency shall be eligible to participate in this program only if the employee is employed at the GS–11 level or above (or equivalent) and is serving under a career or career-conditional appointment or an appointment of equivalent tenure in the excepted service, and applicable requirements of section 209(b) of the E-Government Act of 2002 are met with respect to the proposed assignment of such employee.

(b) Agreements**.—** Each agency that exercises its authority under this chapter shall provide for a written agreement between the agency and the employee concerned regarding the terms and conditions of the employee's assignment. In the case of an employee of the agency, the agreement shall—

(1) require the employee to serve in the civil service, upon completion of the assignment, for a period equal to the length of the assignment; and

(2) provide that, in the event the employee fails to carry out the agreement (except for good and sufficient reason, as determined by the head of the agency from which assigned) the employee shall be liable to the United States for payment of all expenses of the assignment.

An amount under paragraph (2) shall be treated as a debt due the United States.

(c) Termination.— Assignments may be terminated by the agency or private sector organization concerned for any reason at any time.

(d) Duration.— Assignments under this chapter shall be for a period of between 3 months and 1 year, and may be extended in 3-month increments for a total of not more than 1 additional year, except that no assignment under this chapter may commence after the end of the 5-year period beginning on the date of the enactment of this chapter.

(e) Assistance.— The Chief Information Officers Council, by agreement with the Office of Personnel Management, may assist in the administration of this chapter, including by maintaining lists of potential candidates for assignment under this chapter, establishing mentoring relationships for the benefit of individuals who are given assignments under this chapter, and publicizing the program.

(f) Considerations.— In exercising any authority under this chapter, an agency shall take into consideration—

(1) the need to ensure that small business concerns are appropriately represented with respect to the assignments described in sections 3703 and 3704, respectively; and

(2) how assignments described in section 3703 might best be used to help meet the needs of the agency for the training of employees in information technology management.

Sec. 3703. Assignment of employees to private sector organizations

(a) In General.— An employee of an agency assigned to a private sector organization under this chapter is deemed, during the period of the assignment, to be on detail to a regular work assignment in his agency.

(b) Coordination With Chapter 81.— Notwithstanding any other provision of law, an employee of an agency assigned to a private sector organization under this chapter is entitled to retain coverage, rights, and benefits under subchapter I of chapter 81, and employment during the assignment is deemed employment by the United States, except that, if

the employee or the employee's dependents receive from the private sector organization any payment under an insurance policy for which the premium is wholly paid by the private sector organization, or other benefit of any kind on account of the same injury or death, then, the amount of such payment or benefit shall be credited against any compensation otherwise payable under subchapter I of chapter 81.

(c) Reimbursements.— The assignment of an employee to a private sector organization under this chapter may be made with or without reimbursement by the private sector organization for the travel and transportation expenses to or from the place of assignment, subject to the same terms and conditions as apply with respect to an employee of a Federal agency or a State or local government under section 3375, and for the pay, or a part thereof, of the employee during assignment. Any reimbursements shall be credited to the appropriation of the agency used for paying the travel and transportation expenses or pay.

(d) Tort Liability; Supervision.— The Federal Tort Claims Act and any other Federal tort liability statute apply to an employee of an agency assigned to a private sector organization under this chapter. The supervision of the duties of an employee of an agency so assigned to a private sector organization may be governed by an agreement between the agency and the organization.

(e) Small Business Concerns.—

(1) In general.— The head of each agency shall take such actions as may be necessary to ensure that, of the assignments made under this chapter from such agency to private sector organizations in each year, at least 20 percent are to small business concerns.

(2) Definitions.— For purposes of this subsection—

(A) the term "small business concern" means a business concern that satisfies the definitions and standards specified by the Administrator of the Small Business Administration under section 3(a)(2) of the Small Business Act (as from time to time amended by the Administrator);

(B) the term "year" refers to the 12-month period beginning on the date of the enactment of this chapter, and each succeeding 12-month period in which any assignments under this chapter may be made; and

(C) the assignments "made" in a year are those commencing in such year.

(3) Reporting requirement.— An agency which fails to comply with paragraph (1) in a year shall, within 90 days after the end of such year, submit a report to the Committees on Government Reform and Small Business of the House of Representatives and the Committees on Governmental Affairs and Small Business of the Senate. The report shall include—

(A) the total number of assignments made under this chapter from such agency to private sector organizations in the year;

(B) of that total number, the number (and percentage) made to small business concerns; and

(C) the reasons for the agency's noncompliance with paragraph (1).

(4) Exclusion.— This subsection shall not apply to an agency in any year in which it makes fewer than 5 assignments under this chapter to private sector organizations.

3704. Assignment of employees from private sector organizations

(a) In General**.—** An employee of a private sector organization assigned to an agency under this chapter is deemed, during the period of the assignment, to be on detail to such agency.

(b) Terms and Conditions**.—** An employee of a private sector organization assigned to an agency under this chapter—

(1) may continue to receive pay and benefits from the private sector organization from which he is assigned;

(2) is deemed, notwithstanding subsection (a), to be an employee of the agency for the purposes of—

(A) chapter 73;

(B) sections 201, 203, 205, 207, 208, 209, 603, 606, 607, 643, 654, 1905, and 1913 of title 18;

(C) sections 1343, 1344, and 1349 (b) of title 31;

(D) the Federal Tort Claims Act and any other Federal tort liability statute;

(E) the Ethics in Government Act of 1978;

(F) section 1043 of the Internal Revenue Code of 1986; and

(G) section 27 of the Office of Federal Procurement Policy Act;

(3) may not have access to any trade secrets or to any other nonpublic information which is of commercial value to the private sector organization from which he is assigned; and

(4) is subject to such regulations as the President may prescribe. The supervision of an employee of a private sector organization assigned to an agency under this chapter may be governed by agreement between the agency and the private sector organization concerned. Such an assignment may be made with or without reimbursement by the agency for the pay, or a part thereof, of the employee during the period of assignment, or for any contribution of the private sector organization to employee benefit systems.

(c) Coordination With Chapter 81.— An employee of a private sector organization assigned to an agency under this chapter who suffers disability or dies as a result of personal injury sustained while performing duties during the assignment shall be treated, for the purpose of subchapter I of chapter 81, as an employee as defined by section 8101 who had sustained the injury in the performance of duty, except that, if the employee or the employee's dependents receive from the private sector organization any payment under an insurance policy for which the premium is wholly paid by the private sector organization, or other benefit of any kind on account of the same injury or death, then, the amount of such payment or benefit shall be credited against any compensation otherwise payable under subchapter I of chapter 81.

(d) Prohibition Against Charging Certain Costs to the Federal Government.— A private sector organization may not charge the Federal Government, as direct or indirect costs under a Federal contract, the costs of pay or benefits paid by the organization to an employee assigned to an agency under this chapter for the period of the assignment.

3705. Application to Office of the Chief Technology Officer of the District of Columbia

(a) In General**.—** The Chief Technology Officer of the District of Columbia may arrange for the assignment of an employee of the Office of the Chief Technology Officer to a private sector organization, or an employee of a private sector organization to such Office, in the same manner as the head of an agency under this chapter.

(b) Terms and Conditions**.—** An assignment made pursuant to subsection (a) shall be subject to the same terms and conditions as an assignment made by the head of an agency under this chapter, except that in applying such terms and conditions to an assignment made pursuant to subsection (a), any reference in this chapter to a provision of law or regulation of the United States shall be deemed to be a reference to the applicable provision of law or regulation of the District of Columbia, including the applicable provisions of the District of Columbia Government Comprehensive Merit Personnel Act of 1978 (sec. 1–601.01 et seq., D.C. Official Code) and section 601 of the District of Columbia Campaign Finance Reform and Conflict of Interest Act (sec. 1–1106.01, D.C. Official Code).

(c) Definition.— For purposes of this section, the term "Office of the Chief Technology Officer" means the office established in the executive branch of the government of the District of Columbia under the Office of the Chief Technology Officer Establishment Act of 1998 (sec. 1–1401 et seq., D.C. Official Code).

3706. Reporting requirement

(a) In General.— The Office of Personnel Management shall, not later than April 30 and October 31 of each year, prepare and submit to the Committee on Government Reform of the House of

Representatives and the Committee on Governmental Affairs of the Senate a semiannual report summarizing the operation of this chapter during the immediately preceding 6-month period ending on March 31 and September 30, respectively.

(b) Content.— Each report shall include, with respect to the 6-month period to which such report relates—

(1) the total number of individuals assigned to, and the total number of individuals assigned from, each agency during such period;

(2) a brief description of each assignment included under paragraph (1), including—

(A) the name of the assigned individual, as well as the private sector organization and the agency (including the specific bureau or other agency component) to or from which such individual was assigned;

(B) the respective positions to and from which the individual was assigned, including the duties and responsibilities and the pay grade or level associated with each; and

(C) the duration and objectives of the individual's assignment; and

(3) such other information as the Office considers appropriate.

(c) Publication.— A copy of each report submitted under subsection (a)—

(1) shall be published in the Federal Register; and

(2) shall be made publicly available on the Internet.

(d) Agency Cooperation.— On request of the Office, agencies shall furnish such information and reports as the Office may require in order to carry out this section.

3707. Regulations

The Director of the Office of Personnel Management shall prescribe regulations for the administration of this chapter.

TITLE 10 – SUBTITLE A – PART IV – CHAPTER 137 – PROCUREMENT GENERALLY

Sec. 2332. Share-in-savings contracts

(a) Authority To Enter Into Share-in-Savings Contracts.—

(1) The head of an agency may enter into a share-in-savings contract for information technology (as defined in section 11101 (6) of title 40) in which the Government awards a contract to improve mission-related or administrative processes or to accelerate the achievement of its mission and share with the contractor in savings achieved through contract performance.

(2) (A) Except as provided in subparagraph (B), a share-in-savings contract shall be awarded for a period of not more than five years.

(B) A share-in-savings contract may be awarded for a period greater than five years, but not more than 10 years, if the head of the agency determines in writing prior to award of the contract that—

(i) the level of risk to be assumed and the investment to be undertaken by the contractor is likely to inhibit the government from obtaining the needed information technology competitively at a fair and reasonable price if the contract is limited in duration to a period of five years or less; and

(ii) usage of the information technology to be acquired is likely to continue for a period of time sufficient to generate reasonable benefit for the government.

(3) Contracts awarded pursuant to the authority of this section shall, to the maximum extent practicable, be performance-based contracts that identify objective outcomes and contain performance standards that will be used to measure achievement and milestones that must be met before payment is made.

(4) Contracts awarded pursuant to the authority of this section shall include a provision containing a quantifiable baseline that is to be the basis upon which a savings share ratio is established that governs the amount of payment a contractor is to receive under the contract. Before commencement of performance of such a contract,

the senior procurement executive of the agency shall determine in writing that the terms of the provision are quantifiable and will likely yield value to the Government.

(5) (A) The head of the agency may retain savings realized through the use of a share-in-savings contract under this section that are in excess of the total amount of savings paid to the contractor under the contract, but may not retain any portion of such savings that is attributable to a decrease in the number of civilian employees of the Federal Government performing the function. Except as provided in subparagraph (B), savings shall be credited to the appropriation or fund against which charges were made to carry out the contract and shall be used for information technology.

(B) Amounts retained by the agency under this subsection shall—

(i) without further appropriation, remain available until expended; and

(ii) be applied first to fund any contingent liabilities associated with share-in-savings procurements that are not fully funded.

(b) Cancellation and Termination.—

(1) If funds are not made available for the continuation of a share-in-savings contract entered into under this section in a subsequent fiscal year, the contract shall be canceled or terminated. The costs of cancellation or termination may be paid out of—

(A) appropriations available for the performance of the contract;

(B) appropriations available for acquisition of the information technology procured under the contract, and not otherwise obligated; or

(C) funds subsequently appropriated for payments of costs of cancellation or termination, subject to the limitations in paragraph (3).

(2) The amount payable in the event of cancellation or termination of a share-in-savings contract shall be negotiated with the contractor at the time the contract is entered into.

(3) (A) Subject to subparagraph (B), the head of an agency may enter into share-in-savings contracts under this section in any given fiscal year

even if funds are not made specifically available for the full costs of cancellation or termination of the contract if funds are available and sufficient to make payments with respect to the first fiscal year of the contract and the following conditions are met regarding the funding of cancellation and termination liability:

(i) The amount of unfunded contingent liability for the contract does not exceed the lesser of—

(I) 25 percent of the estimated costs of a cancellation or termination; or

(II) $5,000,000.

(ii) Unfunded contingent liability in excess of $1,000,000 has been approved by the Director of the Office of Management and Budget or the Director's designee.

(B) The aggregate number of share-in-savings contracts that may be entered into under subparagraph (A) by all agencies to which this chapter applies in a fiscal year may not exceed 5 in each of fiscal years 2003, 2004, and 2005.

(c) Definitions.— In this section:

(1) The term "contractor" means a private entity that enters into a contract with an agency.

(2) The term "savings" means—

(A) monetary savings to an agency; or

(B) savings in time or other benefits realized by the agency, including enhanced revenues (other than enhanced revenues from the collection of fees, taxes, debts, claims, or other amounts owed the Federal Government).

(3) The term "share-in-savings contract" means a contract under which—

(A) a contractor provides solutions for—

(i) improving the agency's mission-related or administrative processes; or

(ii) accelerating the achievement of agency missions; and

(B) the head of the agency pays the contractor an amount equal to a portion of the savings derived by the agency from—

(i) any improvements in mission-related or administrative processes that result from implementation of the solution; or

(ii) acceleration of achievement of agency missions.

(d) Termination.— No share-in-savings contracts may be entered into under this section after September 30, 2005.

TITLE 41 – CHAPTER 4 – SUBCHAPTER IV – PROCUREMENT PROVISIONS

Sec. 266a. Share-in-savings contracts

(a) Authority to enter into share-in-savings contracts

(1) The head of an executive agency may enter into a share-in-savings contract for information technology (as defined in section 11101 (6) of title 40) in which the Government awards a contract to improve mission-related or administrative processes or to accelerate the achievement of its mission and share with the contractor in savings achieved through contract performance.

(2) (A) Except as provided in subparagraph (B), a share-in-savings contract shall be awarded for a period of not more than five years.

(B) A share-in-savings contract may be awarded for a period greater than five years, but not more than 10 years, if the head of the agency determines in writing prior to award of the contract that—

(i) the level of risk to be assumed and the investment to be undertaken by the contractor is likely to inhibit the government from obtaining the needed information technology competitively at a fair and reasonable price if the contract is limited in duration to a period of five years or less; and

(ii) usage of the information technology to be acquired is likely to continue for a period of time sufficient to generate reasonable benefit for the government.

(3) Contracts awarded pursuant to the authority of this section shall, to the maximum extent practicable, be performance-based contracts that identify objective outcomes and contain performance standards that will be used to measure achievement and milestones that must be met before payment is made.

(4) Contracts awarded pursuant to the authority of this section shall include a provision containing a quantifiable baseline that is to be the basis upon which a savings share ratio is established that governs the amount of payment a contractor is to receive under the contract. Before commencement of performance of such a contract, the senior procurement executive of the agency shall determine in writing that the terms of the provision are quantifiable and will likely yield value to the Government.

(5) (A) The head of the agency may retain savings realized through the use of a share-in-savings contract under this section that are in excess of the total amount of savings paid to the contractor under the contract, but may not retain any portion of such savings that is attributable to a decrease in the number of civilian employees of the Federal Government performing the function. Except as provided in subparagraph (B), savings shall be credited to the appropriation or fund against which charges were made to carry out the contract and shall be used for information technology.

(B) Amounts retained by the agency under this subsection shall—

(i) without further appropriation, remain available until expended; and

(ii) be applied first to fund any contingent liabilities associated with share-in-savings procurements that are not fully funded.

(b) Cancellation and termination

(1) If funds are not made available for the continuation of a share-in-savings contract entered into under this section in a subsequent fiscal year, the contract shall be canceled or terminated. The costs of cancellation or termination may be paid out of—

(A) appropriations available for the performance of the contract;

(B) appropriations available for acquisition of the information technology procured under the contract, and not otherwise obligated; or

(C) funds subsequently appropriated for payments of costs of cancellation or termination, subject to the limitations in paragraph (3).

(2) The amount payable in the event of cancellation or termination of a share-in-savings contract shall be negotiated with the contractor at the time the contract is entered into.

(3) (A) Subject to subparagraph (B), the head of an executive agency may enter into share-in-savings contracts under this section in any given fiscal year even if funds are not made specifically available for the full costs of cancellation or termination of the contract if funds are available and sufficient to make payments with respect to the first fiscal year of the contract and the following conditions are met regarding the funding of cancellation and termination liability:

(i) The amount of unfunded contingent liability for the contract does not exceed the lesser of—

(I) 25 percent of the estimated costs of a cancellation or termination; or

(II) $5,000,000.

(ii) Unfunded contingent liability in excess of $1,000,000 has been approved by the Director of the Office of Management and Budget or the Director's designee.

(B) The aggregate number of share-in-savings contracts that may be entered into under subparagraph (A) by all executive agencies to which this subchapter [1] applies in a fiscal year may not exceed 5 in each of fiscal years 2003, 2004, and 2005.

(c) Definitions

In this section:

(1) The term "contractor" means a private entity that enters into a contract with an agency.

(2) The term "savings" means—

(A) monetary savings to an agency; or

(B) savings in time or other benefits realized by the agency, including enhanced revenues (other than enhanced revenues from the collection of fees, taxes, debts, claims, or other amounts owed the Federal Government).

(3) The term "share-in-savings contract" means a contract under which—

(A) a contractor provides solutions for—

(i) improving the agency's mission-related or administrative processes; or

(ii) accelerating the achievement of agency missions; and

(B) the head of the agency pays the contractor an amount equal to a portion of the savings derived by the agency from—

(i) any improvements in mission-related or administrative processes that result from implementation of the solution; or

(ii) acceleration of achievement of agency missions.

(d) Termination

No share-in-savings contracts may be entered into under this section after September 30, 2005.

TITLE 40 – SUBTITLE I – CHAPTER 5 – SUBCHAPTER I – PROCUREMENT AND WAREHOUSING

Sec. 502. Services for other entities

(c) Use of Certain Supply Schedules.—

(1) In general.— The Administrator may provide for the use by State or local governments of Federal supply schedules of the General Services Administration for automated data processing equipment (including firmware), software, supplies, support equipment, and services (as contained in Federal supply classification code group 70).

(2) Voluntary use.— In any case of the use by a State or local government of a Federal supply schedule pursuant to paragraph (1),

participation by a firm that sells to the Federal Government through the supply schedule shall be voluntary with respect to a sale to the State or local government through such supply schedule.

(3) Definitions.— In this subsection:

(A) The term "State or local government" includes any State, local, regional, or tribal government, or any instrumentality thereof (including any local educational agency or institution of higher education).

(B) The term "tribal government" means—

(i) the governing body of any Indian tribe, band, nation, or other organized group or community located in the continental United States (excluding the State of Alaska) that is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians, and

(ii) any Alaska Native regional or village corporation established pursuant to the Alaska Native Claims Settlement Act (43 U.S.C. 1601 et seq.).

(C) The term "local educational agency" has the meaning given that term in section 8013 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7713). (D) The term "institution of higher education" has the meaning given that term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001 (a)).

TITLE 44 – CHAPTER 35 – SUBCHAPTER III – INFORMATION SECURITY

Sec. 3541. Purposes

The purposes of this subchapter are to—

(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

(4) provide a mechanism for improved oversight of Federal agency information security programs;

(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and

(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

Sec. 3542. Definitions

(a) In General.— Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

(b) Additional Definitions.— As used in this subchapter:

(1) The term “information security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(A) integrity, which means guarding against improper informationmodification or destruction, and includes ensuring information nonrepudiation and authenticity;

(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(C) availability, which means ensuring timely and reliable access to and use of information.

(2) (A) The term “national security system” means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(i) the function, operation, or use of which—

(I) involves intelligence activities;

(II) involves cryptologic activities related to national security;

(III) involves command and control of military forces;

(IV) involves equipment that is an integral part of a weapon or weapons system; or

(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(3) The term “information technology” has the meaning given that term in section 11101 of title 40.

Sec. 3543. Authority and functions of the Director

(a) In General.— The Director shall oversee agency information security policies and practices, including—

(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of—

(A) information collected or maintained by or on behalf of an agency; or

(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(3) coordinating the development of standards and guidelines 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) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

(4) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements;

(5) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3544 (b);

(6) coordinating information security policies and procedures with related information resources management policies and procedures;

(7) overseeing the operation of the Federal information security incident center required under section 3546; and

(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including—

(A) a summary of the findings of evaluations required by section 3545;

(B) an assessment of the development, promulgation, and adoption of, and compliance with, standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and promulgated under section 11331 of title 40;

(C) significant deficiencies in agency information security practices;

(D) planned remedial action to address such deficiencies; and

(E) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(d)(10) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

(b) National Security Systems.— Except for the authorities described in paragraphs (4) and (8) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

(c) Department of Defense and Central Intelligence Agency Systems.—

(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of Central Intelligence in the case of systems described in paragraph (3).

(2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

(3) The systems described in this paragraph are systems that are operated by the Central Intelligence Agency, a contractor of the Central

Intelligence Agency, or another entity on behalf of the Central Intelligence Agency that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Central Intelligence Agency.

Sec. 3544. Federal agency responsibilities

(a) In General.— The head of each agency shall—

(1) be responsible for—

(A) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

(i) information collected or maintained by or on behalf of the agency; and

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(B) complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including—

(i) information security standards promulgated under section 11331 of title 40; and

(ii) information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

(C) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—

(A) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

(B) determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;

(C) implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including—

(A) designating a senior agency information security officer who shall—

(i) carry out the Chief Information Officer's responsibilities under this section;

(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

(iii) have information security duties as that official's primary duty; and

(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

(B) developing and maintaining an agencywide information security program as required by subsection (b);

(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3543 of this title, and section 11331 of title 40;

(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

(b) Agency Program.— Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3543 (a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

(2) policies and procedures that—

(A) are based on the risk assessments required by paragraph (1);

(B) cost-effectively reduce information security risks to an acceptable level;

(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

(D) ensure compliance with—

(i) the requirements of this subchapter;

(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;

(iii) minimally acceptable system configuration requirements, as determined by the agency; and

(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—

(A) information security risks associated with their activities; and

(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—

(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505 (c); and

(B) may include testing relied on in a[7] evaluation under section 3545;

(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

(7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546 (b), including—

[7] So in original. Probably should be “an”.

(A) mitigating risks associated with such incidents before substantial damage is done;

(B) notifying and consulting with the Federal information security incident center referred to in section 3546; and

(C) notifying and consulting with, as appropriate—

(i) law enforcement agencies and relevant Offices of Inspector General;

(ii) an office designated by the President for any incident involving a national security system; and

(iii) any other agency or office, in accordance with law or as directed by the President; and

(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

(c) Agency Reporting.— Each agency shall—

(1) report annually to the Director, the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter, including compliance with each requirement of subsection (b);

(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

(A) annual agency budgets;

(B) information resources management under subchapter 1[8] of this chapter;

(C) information technology management under subtitle III of title 40;

[8] So in original. Probably should be “I”.

(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note ; Public Law 101–576) (and the amendments made by that Act);

(F) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note); and

(G) internal accounting and administrative controls under section 3512 of title 31,[9] (known as the "Federal Managers Financial Integrity Act"); and

(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)—

(A) as a material weakness in reporting under section 3512 of title 31; and

(B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).

(d) Performance Plan.—

(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of—

(A) the time periods, and

(B) the resources, including budget, staffing, and training, that are necessary to implement the program required under subsection (b).

(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1).

(e) Public Notice and Comment.— Each agency shall provide the public with timely notice and opportunities for comment on proposed

[9] So in original. The comma probably should not appear.

information security policies and procedures to the extent that such policies and procedures affect communication with the public.

Sec. 3545. Annual independent evaluation

(a) In General.—

(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

(2) Each evaluation under this section shall include—

(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

(B) an assessment (made on the basis of the results of the testing) of compliance with—

(i) the requirements of this subchapter; and

(ii) related information security policies, procedures, standards, and guidelines; and

(C) separate presentations, as appropriate, regarding information security relating to national security systems.

(b) Independent Auditor.— Subject to subsection (c)—

(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978 or any other law, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

(2) for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

(c) National Security Systems.— For each agency operating or exercising control of a national security system, that portion of the

evaluation required by this section directly relating to a national security system shall be performed—

(1) only by an entity designated by the agency head; and

(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

(d) Existing Evaluations.— The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

(e) Agency Reporting.—

(1) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

(2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

(f) Protection of Information.— Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

(g) OMB Reports to Congress.—

(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3543 (a)(8).

(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of Central Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

(h) Comptroller General.— The Comptroller General shall periodically evaluate and report to Congress on—

(1) the adequacy and effectiveness of agency information security policies and practices; and

(2) implementation of the requirements of this subchapter.

Sec. 3546. Federal information security incident center

(a) In General.— The Director shall ensure the operation of a central Federal information security incident center to—

(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

(2) compile and analyze information about incidents that threaten information security;

(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities; and

(4) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

(b) National Security Systems.— Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center

to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

Sec. 3547. National security systems

The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency—

(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;

(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

(3) complies with the requirements of this subchapter.

Sec. 3548. Authorization of appropriations

There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.

Sec. 3549. Effect on existing law

Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards[10] and Technology Act (15 U.S.C. 278g–3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title,

[10] So in original. Probably should be "National Institute of Standards".

or the disclosure of information to the Congress or the Comptroller General of the United States. While this subchapter is in effect, subchapter II of this chapter shall not apply.

TITLE 40— SUBTITLE III—CHAPTER 113—SUBCHAPTER III

Sec. 11331. Responsibilities for Federal information systems standards.[11]

---

[11] Amendments – Pub. L. 107–296 amended text generally. Prior to amendment, text, as amended generally by Pub. L. 107–347, Electronic Government Act of 2002, read as follows:
"(a) Standards and Guidelines.—
"(1) Authority to prescribe.—Except as provided under paragraph (2), the Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3 (a)), prescribe standards and guidelines pertaining to Federal information systems.
"(2) National security systems.—Standards and guidelines for national security systems (as defined under this section) shall be developed, prescribed, enforced, and overseen as otherwise authorized by law and as directed by the President.
"(b) Mandatory Requirements.—
"(1) Authority to make mandatory.—Except as provided under paragraph (2), the Secretary shall make standards prescribed under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of Federal information systems.
"(2) Required mandatory standards.—(A) Standards prescribed under subsection (a)(1) shall include information security standards that—
"(i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3 (b)); and
"(ii) are otherwise necessary to improve the security of Federal information and information systems.
"(B) Information security standards described in subparagraph (A) shall be compulsory and binding.
"(c) Authority to Disapprove or Modify.—The President may disapprove or modify the standards and guidelines referred to in subsection (a)(1) if the President determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

(a) Definition.— In this section, the term "information security" has the meaning given that term in section 3532 (b)(1) of title 44.

(b) Requirement to Prescribe Standards.—

(1) In general.—

(A) Requirement.— Except as provided under paragraph (2), the Director of the Office of Management and Budget shall, on the basis of proposed standards developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3 (a)) and in consultation with the Secretary of Homeland Security, promulgate information security standards pertaining to Federal information systems.

(B) Required standards.— Standards promulgated under subparagraph

(A) shall include—

"(d) Exercise of Authority.—To ensure fiscal and policy consistency, the Secretary shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director of the Office of Management and Budget.
"(e) Application of More Stringent Standards.—The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards the Secretary prescribes under this section if the more stringent standards—
"(1) contain at least the applicable standards made compulsory and binding by the Secretary; and
"(2) are otherwise consistent with policies and guidelines issued under section 3543 of title 44.
"(f) Decisions on Promulgation of Standards.—The decision by the Secretary regarding the promulgation of any standard under this section shall occur not later than 6 months after the submission of the proposed standard to the Secretary by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).
"(g) Definitions.—In this section:
"(1) Federal information system.—The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
"(2) Information security.—The term 'information security' has the meaning given that term in section 3542 (b)(1) of title 44.
"(3) National security system.—The term 'national security system' has the meaning given that term in section 3542 (b)(2) of title 44."

(i) standards that provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3 (b)); and

(ii) such standards that are otherwise necessary to improve the efficiency of operation or security of Federal information systems.

(C) Required standards binding.— Information security standards described under subparagraph (B) shall be compulsory and binding.

(2) Standards and guidelines for national security systems.— Standards and guidelines for national security systems, as defined under section 3532 (3) of title 44, shall be developed, promulgated, enforced, and overseen as otherwise authorized by law and as directed by the President.

(c) Application of More Stringent Standards.— The head of an agency may employ standards for the cost-effective information security for all operations and assets within or under the supervision of that agency that are more stringent than the standards promulgated by the Director under this section, if such standards—

(1) contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Director; and

(2) are otherwise consistent with policies and guidelines issued under section 3533 of title 44.

(d) Requirements Regarding Decisions by Director.—

(1) Deadline.— The decision regarding the promulgation of any standard by the Director under subsection (b) shall occur not later than 6 months after the submission of the proposed standard to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

(2) Notice and comment.— A decision by the Director to significantly modify, or not promulgate, a proposed standard submitted to the Director by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), shall be made after the public is given an opportunity to comment on the Director's proposed decision.

TITLE 15 – CHAPTER 7 – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Sec. 278g–3. Computer standards program

(a) In general

The Institute shall—

(1) have the mission of developing standards, guidelines, and associated methods and techniques for information systems;

(2) develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems (as defined in section 3532 (b)(2) of title 44);

(3) develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems; and

(4) carry out the responsibilities described in paragraph (3) through the Computer Security Division.

(b) Minimum requirements for standards and guidelines

The standards and guidelines required by subsection (a) of this section shall include, at a minimum—

(1) (A) standards to be used by all agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;

(B) guidelines recommending the types of information and information systems to be included in each such category; and

(C) minimum information security requirements for information and information systems in each such category;

(2) a definition of and guidelines concerning detection and handling of information security incidents; and

(3) guidelines developed in coordination with the National Security Agency for identifying an information system as a national security system consistent with applicable requirements for national security systems, issued in accordance with law and as directed by the President.

(c) Development of standards and guidelines

In developing standards and guidelines required by subsections (a) and (b) of this section, the Institute shall—

(1) consult with other agencies and offices (including, but not limited to, the Director of the Office of Management and Budget, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, and the Secretary of Homeland Security) to assure—

(A) use of appropriate information security policies, procedures, and techniques, in order to improve information security and avoid unnecessary and costly duplication of effort; and

(B) that such standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems;

(2) provide the public with an opportunity to comment on proposed standards and guidelines;

(3) submit to the Director of the Office of Management and Budget for promulgation under section 11331 of title 40—

(A) standards, as required under subsection (b)(1)(A) of this section, no later than 12 months after November 25, 2002; and

(B) minimum information security requirements for each category, as required under subsection (b)(1)(C) of this section, no later than 36 months after November 25, 2002;

(4) issue guidelines as required under subsection (b)(1)(B) of this section, no later than 18 months after November 25, 2002;

(5) ensure that such standards and guidelines do not require specific technological solutions or products, including any specific hardware or software security solutions;

(6) ensure that such standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks; and

(7) use flexible, performance-based standards and guidelines that, to the greatest extent possible, permit the use of off-the-shelf commercially developed information security products.

(d) Information security functions

The Institute shall—

(1) submit standards developed pursuant to subsection (a) of this section, along with recommendations as to the extent to which these should be made compulsory and binding, to the Director of the Office of Management and Budget for promulgation under section 11331 of title 40;

(2) provide assistance to agencies regarding—

(A) compliance with the standards and guidelines developed under subsection (a) of this section;

(B) detecting and handling information security incidents; and

(C) information security policies, procedures, and practices;

(3) conduct research, as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security;

(4) develop and periodically revise performance indicators and measures for agency information security policies and practices;

(5) evaluate private sector information security policies and practices and commercially available information technologies to assess potential application by agencies to strengthen information security;

(6) evaluate security policies and practices developed for national security systems to assess potential application by agencies to strengthen information security;

(7) periodically assess the effectiveness of standards and guidelines developed under this section and undertake revisions as appropriate;

(8) solicit and consider the recommendations of the Information Security and Privacy Advisory Board, established by section 278g–4 of this title, regarding standards and guidelines developed under subsection

(a) of this section and submit such recommendations to the Director of the Office of Management and Budget with such standards submitted to the Director; and

(9) prepare an annual public report on activities undertaken in the previous year, and planned for the coming year, to carry out responsibilities under this section.

(e) Definitions

As used in this section—

(1) the term “agency” has the same meaning as provided in section 3502 (1) of title 44;

(2) the term “information security” has the same meaning as provided in section 3532(1) of such title;

(3) the term “information system” has the same meaning as provided in section 3502(8) of such title;

(4) the term “information technology” has the same meaning as provided in section 11101 of title 40; and

(5) the term “national security system” has the same meaning as provided in section 3532(b)(2) of such title.[12]

Sec. 278g–4. Information Security and Privacy Advisory Board

(a) Establishment and composition

There is hereby established a [13]Information Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

(1) four members from outside the Federal Government who are eminent in the information technology industry, at least one of whom is representative of small or medium sized companies in such industries;

(2) four members from outside the Federal Government who are eminent in the fields of information technology, or related disciplines, but who are not employed by or representative of a producer of information technology; and

(3) four members from the Federal Government who have information system management experience, including experience in information security and privacy, at least one of whom shall be from the National Security Agency.

(b) Duties

The duties of the Board shall be—

(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy;

(2) to advise the Institute and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, including

---

[12] Section 3532(b)(2) of such title, referred to in subsec. (e)(5), probably means section 3532 (b)(2) of title 44.

[13] So in original. Probably should be “an”.

through review of proposed standards and guidelines developed under section 278g–3 of this title; and

(3) to report annually its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress.

(c) Term of office

The term of office of each member of the Board shall be four years, except that—

(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

(d) Quorum

The Board shall not act in the absence of a quorum, which shall consist of seven members.

(e) Allowance for travel expenses Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5.

(f) Meetings The Board shall hold meetings at such locations and at such time and place as determined by a majority of the Board.

(g) Staff services and utilization of Federal personnel

To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the Institute or any other agency of the Federal Government with the consent of the head of the agency.

(h) Definitions

As used in this section, the terms “information system” and “information technology” have the meanings given in section 278g–3 of this title.

DoD Directive 5144.1
Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer (ASD(NII)/DoD CIO)

DoD Directive	5144.1
Date	May 2, 2005
URL	http://www.dtic.mil/whs/directives/corres/html/51441.htm
Editor's note: This assigns chief information officer responsibilities, functions, relationships, and authorities to the Assistant Secretary of Defense for Networks and Information Integration, making the position dual-hatted.	

Reference:

(a) Title 10, United States Code
(b) Title 44, United States Code
(c) Title 40, United States Code
(d) Unified Command Plan, March 1, 2005
(e) through (aa), see enclosure 1

1. PURPOSE

Under the authorities vested in the Secretary of Defense by section 113 of reference (a) and references (b) through (e), this Directive:

1.1. Assigns responsibilities, functions, relationships, and authorities to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO).

1.2. Cancels references (f) through (i).

2. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department

of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

3. RESPONSIBILITIES AND FUNCTIONS

The ASD(NII)/DoD CIO is the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on networks and network-centric policies and concepts; command and control (C2); communications; non-intelligence space matters; enterprise-wide integration of DoD information matters; Information Technology (IT), including National Security Systems (NSS); information resources management (IRM) (as defined by reference (b)); spectrum management; network operations; information systems; information assurance (IA); positioning, navigation, and timing (PNT) policy, including airspace and military-air-traffic control activities; sensitive information integration; contingency support and migration planning; and related matters. Pursuant to chapter 113, subchapter III of 40 U.S.C. (reference (j)), the ASD(NII)/DoD CIO has responsibilities for integrating information and related activities and services across the Department. The ASD(NII)/DoD CIO also serves as the DoD Enterprise-level strategist and business advisor from the information, IT, and IRM perspective; Information and IT architect for the DoD enterprise; and, DoD-wide IT and IRM executive. Hereafter these responsibilities and functions are referred to collectively as "NII and CIO" (including IRM) matters. In the exercise of assigned responsibilities and functions, the ASD(NII)/DoD CIO shall:

3.1. Serve as the senior NII and CIO policy and resources official below the Secretary and Deputy Secretary of Defense.

3.2. Advise and assist the Secretary and Deputy Secretary of Defense on policy and issues regarding all assigned responsibilities and functions as they relate to the Department of Defense.

3.3. As the DoD CIO:

3.3.1. Review and provide recommendations to the Secretary and the Heads of the DoD Components on:

3.3.1.1. The performance of the Department's IT and NSS programs (to include monitoring and evaluating the performance of IT and NSS programs on the basis of all applicable performance measurements).

3.3.1.2. DoD budget requests for IT and NSS pursuant to section 2223 of reference (a).

3.3.1.3. The continuation, modification, or termination of an IT and/or NSS program or project pursuant to section 1425 of reference (c).

3.3.1.4. The continuation, modification, or termination of an NII or CIO program pursuant to the Federal Information Security Management Act of 2002 as part of Public Law (Pub. L.) 107-347 (reference (e)), Executive Order (E.O.). 13011 (reference (k)), and other applicable authorities.

3.3.2. Lead the formulation and implementation of enterprise-level defense strategies from the information, IT, network-centric, and non-intelligence space perspective.

3.3.3. Serve as the information architect for the DoD enterprise information environment, and provide oversight and policy guidance to ensure compliance with standards for developing, maintaining, and implementing sound integrated and interoperable architectures across the Department, including intelligence systems and architectures. Ensure that IA is integrated into architectures pursuant to section 3534 of reference (b) and section 11315 of reference (c).

3.3.4. Perform the duties and fulfill the responsibilities associated with information security and other matters under section 3544 of reference (b).

3.3.5. Serve as the DoD-wide information executive and participate as a member on DoD-wide councils and boards involving NII and CIO matters, including serving as the DoD representative on the Intelligence Community CIO Executive Council.

3.3.6. Ensure that NII and CIO policy and resource decisions are fully responsive to the guidance of the Secretary and Deputy Secretary of Defense.

3.3.7. Develop and maintain the DoD IA program and associated policies, procedures, and standards required by section 2224 of reference (a), chapter 35 of reference (e) and DoD Directive S-3600.1 (reference (l)).

3.3.8. Ensure the interoperability of IT, including NSS, throughout the Department of Defense pursuant to section 2223 of reference (a).

3.3.9. Design and implement, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), the Under Secretary of Defense (Comptroller)/DoD Chief Financial Officer (USD(C)/CFO), the Under Secretary of Defense for Intelligence (USD(I)), and the Chairman of the Joint Chiefs of Staff, a process for maximizing the value and assessing and managing the risks of DoD IT acquisitions, including NSS acquisitions, as applicable.

3.3.10. Ensure compliance with the reduction of information-collection burdens on the public pursuant to section 3507 of reference (b).

3.3.11. Prescribe data and information management policies, procedures, and other guidance for the Department.

3.3.12. Issue policies and procedures necessary to establish and maintain a DoD Records Management Program pursuant to standards, guidelines, and procedures issued under section 2904 of reference (b) and Pub. L. No. 107-347 (reference (e)).

3.3.13. Ensure that IT, including NSS, standards that apply throughout the Department are prescribed and enforced pursuant to section 2223 of reference (a).

3.3.14. Provide advice and other assistance to the Secretary of Defense and other senior DoD managers to ensure that IT, including NSS, is acquired and information resources are managed in a manner consistent with reference (b) and section 11315 of reference (c) as well as the priorities established by the Secretary.

3.3.15. Provide enterprise-wide oversight of the development, integration, and implementation of the Global Information Grid (GIG) in accordance with DoD Directive 8100.1 (reference (m)).

3.3.16. Promote the effective and efficient design and operation of all major IRM processes, including improvements to work processes for the Department pursuant to section 11315 of reference (c).

3.3.17. Provide for the elimination of duplicate IT, including NSS, within and between the DoD Components, including the Military Departments and the Defense Agencies, pursuant to Section 2223 of reference (a).

3.3.18. Maintain a consolidated inventory of DoD 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 pursuant to section 2223 of reference (a).

3.3.19. Provide DoD-wide policy regarding the use of the Internet and web site administration.

3.3.20. Develop policies, in coordination with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), to provide oversight of training, career development, and occupation-specialty programs to ensure that personnel with the requisite knowledge and skills are available to support the DoD Information Enterprise.

3.3.21. Chair the DoD CIO Executive Board.

3.3.22. Establish policies, plans, goals, measures, and baselines to incorporate commercial-off-the-shelf software, knowledge management technologies, and services into the policies, doctrine, and training programs of the Department. Undertake initiatives to increase the use of commercial IT solutions throughout the Department across all applications, including NSS, training, logistics, and non-material solutions.

3.3.23. Serve as the principal DoD official responsible for preparing and defending NII and CIO issues before the Congress as well as

evaluating and assessing Congressional activity for impact on all NII and CIO areas of responsibility.

3.3.24. Provide for the enterprise information environment and ensure that its capabilities are synchronized with requirements. This shall include providing for a common set of Enterprise capabilities that enable users to discover, access, post, process, advertise, retrieve, and fuse data, and make sense of the data gathered.

3.4. With regard to communications and information networks:

3.4.1. Develop and implement network-centric policies, architectures, practices, and processes with emphasis on communications and information networks to enable Defense transformation; however, these do not include content-based communications functions such as those associated with public affairs and public diplomacy.

3.4.2. Identify opportunities presented by communication and information technologies as well as risks and costs, and make recommendations on the initiation of communication and information plans, programs, policies, and procedures accordingly.

3.4.3. Provide policies, oversight, guidance, architecture, and strategic approaches for all communications and information network programs and initiatives on an enterprise-wide basis across the Department, ensuring compliance with the IA requirements as well as interoperability with national and alliance/coalition systems. This includes network-centric and information-integration projects, programs, and demonstrations as they relate to GIG implementation and employment.

3.4.4. Negotiate and conclude international agreements and other arrangements relating to the sharing or exchange of DoD communications equipment, facilities, support, services or other communications resources; the use of DoD electromagnetic spectrum equities; and the use of U.S. communications facilities and/or systems pursuant to DoD Directive 5530.3 (reference (n)). Agreements of an

operational nature within alliance organizations shall be coordinated with the Chairman of the Joint Chiefs of Staff.

3.5. With regard to the electromagnetic spectrum:

3.5.1. Provide policy, oversight, and guidance for all DoD matters related to the electromagnetic spectrum, including the management and use of the electromagnetic spectrum (MUES) pursuant to DoD Directive 4650.1 (reference (o)) and the Electromagnetic Environmental Effects (E3) Program pursuant to DoD Directive 3222.3 (reference (p)) within the Department, nationally, and internationally. Ensure that appropriate national policies for MUES and E3 Control are implemented within the Department pursuant to section 305 and Chapter 8 of title 47, U.S.C. (reference (q)) and the National Telecommunications and Information Administration Manual (reference (r)) as well as applicable international policies and standards.

3.5.2. Serve as the lead within the Department for coordination, approval, and representation of DoD positions on all MUES and E3 Control matters within the U.S. Government as well as in regional, national, and international spectrum-management forums and organizations.

3.5.3. Coordinate, as appropriate, with the Chairman of the Joint Chiefs of Staff regarding the development of electromagnetic spectrum policy.

3.6. With regard to C2:

3.6.1. Develop and integrate the Department's overall C2 strategy, approach, structure, and policies and ensure the C2 structure and architecture are compliant with DoD network-centric precepts, information strategy, and joint needs.

3.6.2. Provide policies, program oversight, guidance, and strategic approaches for all C2 programs and initiatives on an enterprise-wide basis across the Department.

3.6.3. Identify the governance of the C2 structure that addresses the needs of the President and all levels of operational command within the Department.

3.6.4. Oversee and facilitate the integration of national, strategic, operational, and tactical C2 systems/programs, including support to the White House Military Office, pursuant to Secretary of Defense guidance (reference (s)).

3.6.5. Oversee the development and integration of DoD-wide C2 capabilities, including promotion of C2-related research, experimentation, metrics, and analysis techniques.

3.6.6. Direct the Heads of the DoD Components to plan, program, budget, and execute programs that will develop material solutions for Joint Capability Integration and Development System approved joint C2 capabilities.

3.7. With respect to space:

3.7.1. Oversee DoD non-intelligence related space matters, including space-based communications programs, space-based information integration activities, space control activities, operationally responsive space programs, space access, satellite control, space-based position, navigation, and timing programs, environmental sensing, and space launch ranges.

3.7.2. Oversee the Space Major Defense Acquisition Program activities of the DoD Executive Agent for Space in coordination with the USD(AT&L), and in coordination with the USD(I) for space-based intelligence system acquisitions, as delegated by the USD(AT&L).

3.8. With regard to network-centric systems engineering policy and program oversight:

3.8.1. Facilitate and resolve interoperability, performance, and other issues related to interfaces, security, standards, and protocols critical to the end-to-end operation of the GIG.

3.8.2. Oversee a network-centric system engineering effort using facilities and services of the Department of Defense to manage an enterprise-wide technical view for the GIG.

3.8.3. Provide oversight of policies and programs to support independent evaluation and to physically validate the technical performance for key transformational communication programs of the GIG.

3.9. With regard to systems acquisition:

3.9.1 Serve as the Milestone Decision Authority for Major Automated Information Systems and other acquisition programs, as delegated by the USD(AT&L), with responsibility for developing and enforcing the policies and practices of DoD Directive 5000.1 (reference (t)) for such programs, in coordination with the USD(AT&L) and the USD(I), as appropriate.

3.9.2. Provide advice on issues related to all assigned responsibilities and functions to the Defense Acquisition Board and the Defense Space Acquisition Board.

3.10. With regard to PNT:

3.10.1. Develop and implement PNT policy, including airspace and military air traffic control, pursuant to DoD Directive 4650.5 (reference (u)).

3.10.2. Develop and oversee contingency policies regarding the Federal Aviation Administration and its transfer to the Department of Defense under certain national security emergencies, pursuant to E.O. 11161 (reference (v)).

3.11. Support the Special Assistant to the Secretary of Defense and Deputy Secretary of Defense for compartmented activities by coordinating sensitive information integration and providing a support staff and appropriately cleared facilities for these functions pursuant to Deputy Secretary of Defense Memorandum (reference (w)).

3.12. Provide NII and CIO support to the mission of Information Operations in support of DoD Directive S-3600.1 (reference (l)).

3.13. Develop and oversee contingency and crisis response communications policies and planning for stabilization and reconstruction operations carried out by the Department with emphasis given to those executed in concert with the United States Government interagency process, to include the interaction of DoD assets with foreign nations and nongovernmental organizations. Special emphasis shall be placed on migrating technologies uniquely suited to contingency operations that are often not used in DoD applications.

3.14. Participate, pursuant to the responsibilities and functions prescribed herein, in the DoD Planning, Programming, Budgeting, and Execution process, which includes proposing DoD programs, formulating budget estimates, recommending resource allocations and priorities, and monitoring the implementation of approved programs in order to ensure adherence to approved policy and planning guidance. This includes conducting program evaluation, assessments, and cross-program reviews, when applicable.

3.15. Address issues associated with meteorology, oceanography, and space weather programs (METOC) and provide overall guidance on DoD METOC matters. Ensure that DoD METOC systems and architectures are interoperable and consistent with GIG policies.

3.16. Address international issues associated with information and communications technologies, including technologies for the non-automatic movement, transmission, or reception of information. Negotiate and conclude international agreements relating to coalition command, control, and communications (C3) and IT policies, standards, and programs pursuant to DoD Directive 5530.3 (reference (n)). Exercise authority, direction, and control and approval of U.S. representation and negotiating positions in international fora and the

conclusion of international agreements related to coalition C3 and international IT policies, standards, and programs.

3.17. Represent the Secretary of Defense at the North Atlantic Treaty Organization C3 Board.

3.18. Recommend changes to the Director, Program Analysis and Evaluation regarding to the content of the "virtual" Major Force Program for the GIG.

3.19. Serve on boards, committees, and other groups and represent the Secretary and Deputy Secretary of Defense on matters outside the Department pursuant to responsibilities and functions prescribed herein.

3.20. Periodically review assigned DoD Executive Agent responsibilities and functions to ensure conformance with DoD Directive 5101.1 (reference (x)).

3.21. Identify and convey enterprise-wide, information-related research requirements to the Director of Defense Research and Engineering (DDR&E) and other Senior Officials in the Department, as appropriate. In coordination and consultation with the DDR&E, establish reliability, survivability, and endurability design criteria/standards for DoD C3 and develop and maintain a technology investment strategy to support the development, acquisition, and integration of DoD C3 services, systems, and processes.

3.22. Provide advice on issues related to all assigned responsibilities and functions to the Joint Requirements Oversight Council and Joint Capabilities Integration and Development System process.

3.23. Coordinate with the USD(I) to ensure that intelligence systems and architectures for collection, analysis, and dissemination of critical intelligence information follow net-centric strategies and are consistent and interoperable with DoD command, control, and communications and information-enterprise systems.

3.24. Coordinate with the Assistant Secretary of Defense for Homeland Defense to ensure interoperability of information systems with non-DoD organizations for homeland security and homeland defense.

3.25. Coordinate with the USD(AT&L) as the Vice Chair of the Defense Business Systems Management Committee to ensure that business systems and architectures for collection, analysis, and dissemination of militarily relevant information are consistent and interoperable with DoD command, control, communications, and information-enterprise systems.

3.26. Ensure that NII and CIO policies and programs are designed and managed in ways that improve standards of performance, economy, and efficiency and that all Defense Agencies and DoD Field Activities under the authority, direction, and control of the ASD(NII)/DoD CIO are attentive and responsive to the requirements of their organizational customers, internal and external to the Department.

3.27. Perform other such duties as the Secretary or Deputy Secretary of Defense may direct.

4. RELATIONSHIPS

4.1. In the performance of all assigned responsibilities and functions, the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer shall:

4.1.1. Report directly to the Secretary and Deputy Secretary of Defense.

4.1.2. Oversee and exercise authority, direction, and control over the Director, Defense Information Systems Agency.

4.1.3. In consultation and coordination with the USD(I), provide policy guidance to the Director, National Security Agency regarding network operations and IA matters.

4.1.4. Use existing facilities and services of the Department of Defense and other Federal Agencies, whenever practicable, to avoid duplication and achieve maximum efficiency and economy.

4.1.5. Provide advice to the OSD Principal Staff Assistants, as necessary, on DoD-wide issues associated with IRM, requirements analysis, budget-preparation matters, reporting activities, Congressional material, and enterprise architectural design related to those areas under the cognizance of the ASD(NII)/DoD CIO.

4.1.6. Serve as the sponsor of the Command, Control, Communications, and Intelligence Federally Funded Research and Development Center.

4.2. The Secretaries of the Military Departments shall provide timely advice to the ASD(NII)/DoD CIO and shall ensure that the policies and guidance issued by the ASD(NII)/DoD CIO are implemented in their respective Military Departments.

4.3. The Heads of the DoD Components shall coordinate with the ASD(NII)/DoD CIO on all matters relating to the responsibilities and functions cited in section 3, above.

5. AUTHORITIES

The ASD(NII)/DoD CIO is hereby delegated authority to:

5.1. Issue DoD Instructions, DoD publications, and one-time directive-type memoranda, consistent with DoD 5025.1-M (reference (y)), that implement policy approved by the Secretary or Deputy Secretary of Defense in the areas of assigned responsibilities and functions. Instructions to the Military Departments shall be issued through the Secretaries of the Military Departments, or their designees.

5.2. Obtain reports, information, advice, and assistance, consistent with DoD Directive 8910.1 (reference (z)) and DoD Directive 8000.1 (reference (aa)), as necessary, to carry out assigned functions.

5.3. Communicate directly with the Heads of the DoD Components. Communications with the Military Departments shall be transmitted through the Secretaries of the Military Departments, their designees, or as otherwise provided in law or directed by the Secretary or Deputy Secretary of Defense in other DoD issuances, or except as provided in paragraph 5.4. below. Communications to the Commanders of the Combatant Commands, except in unusual circumstances, shall be transmitted through the Chairman of the Joint Chiefs of Staff. With the concurrence of the Chairman of the Joint Chiefs of Staff and the cognizant Combatant Commander, Chief Information Officers of the Combatant Commands may directly contact the ASD(NII)/DoD CIO or designee, when required.

5.4. Communicate directly with the CIOs of the DoD Components on all matters for which the ASD(NII)/DoD CIO is assigned responsibilities herein.

5.5. Establish arrangements for DoD participation in non-Defense governmental programs for which the ASD(NII)/DoD CIO is assigned primary responsibility.

5.6. Represent the Department of Defense and represent the Secretary and Deputy Secretary of Defense on matters prescribed herein with government agencies, representatives of the legislative branch, members of the public, and representatives of foreign governments and international organizations, as appropriate, in carrying out assigned responsibilities and functions.

5.7. Exercise the specific delegations of authority in enclosure 2.

6. EFFECTIVE DATE

This Directive is effective immediately.

Enclosures - 2

E1. References, continued

E2. Delegations of Authority

E1. ENCLOSURE 1

REFERENCES, continued

(e) E-Government Act of 2002 (Public Law 107-347), December 17, 2002

(f) DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I))," February 12, 1992 (hereby canceled)

(g) Deputy Secretary of Defense Memorandum, "Establishment of the Deputy Under Secretary of Defense for Space Acquisition and Technology Programs," December 10, 1994 (hereby canceled)

(h) Deputy Secretary of Defense Memorandum, "Responsibilities and Functions of the Deputy Under Secretary of Defense for Space," March 8, 1995 (hereby canceled)

(i) Secretary of Defense Memorandum, "Implementation of Subdivision E of the Clinger- Cohen Act of 1996 (Pub. L. No. 104-106)," June 2, 1997 (hereby canceled)

(j) Chapter 113, Subchapter III of title 40, United States Code

(k) Executive Order 13011, "Federal Information Technology," July 16, 1996

(l) DoD Directive S-3600.1, "Information Operations," December 9, 1996

(m) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 9, 2002

(n) DoD Directive 5530.3, "International Agreements," June 11, 1987

(o) DoD Directive 4650.1, "Policy for Management and Use of the Electromagnetic Spectrum," June 8, 2004

(p) DoD Directive 3222.3, "DoD Electromagnetic Environmental Effects (E3) Program," September 8, 2004

(q) Section 305 and Chapter 8, title 47, United States Code

(r) Part 300, title 47, Code of Federal Regulations (U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA), "Manual of Regulations and Procedures for Federal Radio Frequency Management)

(s) Secretary of Defense Memorandum, "Secretary of Defense Executive Agent for DoD Assets Supporting White House Military Office (WHMO)," February 17, 1999 (classified)

(t) DoD Directive 5000.1, "The Defense Acquisition System," May 12, 2003

(u) DoD Directive 4650.5, "Positioning, Navigation, and Timing," June 2, 2003

(v) Executive Order 11161, "Relating to Certain Relationships Between the Department of Defense and the Federal Aviation Administration," July 7, 1964, as amended by Executive Order 11382

(w) Deputy Secretary of Defense Memorandum, October 10, 2003 (subject and content are classified)

(x) DoD Directive 5101.1, "DoD Executive Agent," September 3, 2002

(y) DoD 5025.1-M, "DoD Directives System Procedures," current edition

(z) DoD Directive 8910.1, "Management and Control of Information Requirements," June 11, 1993

(aa) DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," February 27, 2002

Requests for copies can be forwarded to the Director, NII Administration and Management, Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, and will be provided based upon DoD policy and a need to know regarding classified information.

E2. ENCLOSURE 2

DELEGATIONS OF AUTHORITY

E2.1.1. Pursuant to the authority vested in the Secretary of Defense, and subject to the authority, direction, and control of the Secretary of Defense, and in accordance with DoD policies, Directives, and Instructions, the ASD(NII)/DoD CIO, or the person acting for the ASD(NII)/DoD CIO in his or her absence, is hereby delegated authority, as required, in the administration and operation of the Office of the ASD(NII)/DoD CIO to:

E2.1.1.1. Perform the duties and fulfill the responsibilities of the Secretary of Defense under sections 11312 and 11313 of title 40, United States Code. Assist the USD(Comptroller)/ DoD Chief Financial Officer in performing and fulfilling the responsibilities of the Secretary of Defense under section 11316 of title 40, United States Code.

E2.1.1.2. Make original security classification determinations (up to and including top secret) in accordance with E.O. 12958, "Classified National Security Information," April 17, 1995.

E2.1.1.3. Make written determinations for the conduct of all closed meetings of Federal Advisory Committees under the cognizance of the ASD(NII)/DoD CIO as prescribed by section 10(d) of the Federal Advisory Committee Act (5 U.S.C. Appendix II, 10(d)).

E2.1.2. The ASD(NII)/DoD CIO may redelegate these authorities, as appropriate, and in writing, except as otherwise specifically indicated above or prohibited by law, Directive, or regulation.

DoD Directive 8000.1, Management of DoD Information Resources and Information Technology

DoD Directive	8000.1, Management of DoD Information Resources and Information Technology
Date	February 27, 2002
URL	http://www.dtic.mil/whs/directives/corres/html/80001.htm
Editor's note: This establishes CIO policies and authorities in the Department of Defense, in accordance with law and other policies in DoD. It also requires each DoD Component, including the Military Departments, to have a CIO reporting directly to the Component Head. A reissuance on March 20, 2002, incorporated an administrative change.	

References: (a) DoD Directive 7740.1, "DoD Information Resources Management Program," June 20, 1983 (hereby canceled)
(b) DoD 7740.1-G, "Department of Defense ADP Internal Control Guideline," July 19, 1988 (hereby canceled)
(c) DoD Directive 8000.1, "Defense Information Management (IM) Program," October 27, 1992 (hereby canceled)
(d) Public Law 104-13, "Paperwork Reduction Act" (Chapter 35 of title 44, United States Code)
(e) through (n), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Cancels references (a) and (b).

1.2. Reissues reference (c) to implement references (d), (e), (f), (g), and (h).

1.3. Establishes policies for DoD information resources management (IRM), including information technology (IT), and delineates authorities, duties, and responsibilities for DoD IRM activities consistent with reference (i)

1.4. Provides direction on establishing Chief Information Officers (CIOs) at various levels consistent with reference (e).

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to:

2.1.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.1.2. All phases and activities of the information life cycle regardless of medium or intended use within the Department.

2.1.3. All DoD IT, including IT in National Security Systems (NSS).

2.2. This Directive does not change or otherwise affect information release or disclosure requirements imposed by the Arms Export Control Act, the Privacy Act, the Freedom of Information Act, and Sections 2320 and 2321 of title 10, United States Code.

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Each DoD Component shall have a CIO who reports directly to the Head of the Component, and who shall head an office responsible for ensuring that the DoD Component complies with and promptly, efficiently, and effectively implements information policies and IRM responsibilities in this Directive.

4.2. CIOs may be designated at sub-Component levels.

4.3. Forums shall be established to:

4.3.1. Exchange views and solidify relationships between the DoD Component CIO, and the Joint Community CIO (reference (j)) and other senior managers (e.g., functional managers, Acquisition Executives, Comptrollers).

4.3.2. Identify and establish IRM best practices.

4.3.3. Resolve issues to effectively and efficiently manage information and the technology that supports it.

4.4. Accurate and consistent information shall be available to decision-makers so they can effectively execute the DoD mission. Accordingly:

4.4.1. The function or activity shall determine the need for and availability of information.

4.4.2. Data and information shall be structured to enable full interoperability and integration across DoD operations and activities. Creation of duplicate data shall be minimized and to the extent possible data shall be entered only once. This increases data accuracy, decreases the need for resources to reconcile data from several sources, and promotes data sharing.

4.4.3. An integrated DoD architecture with operational, system, and technical views shall be developed, maintained, and applied to determine interoperability and capability requirements, promote standards, accommodate the accessibility and usability requirements of reference (k), and implement security requirements across the DoD enterprise to provide the basis for efficient and effective acquisition and operation of IT capabilities.

4.4.4. Where workable and cost effective, the DoD Components shall use DoD-wide automated information systems (AIS) and software applications. These AIS shall be designed to use common or enterprise networks, data centers, computing hardware, and databases.

4.4.5. The DoD Components shall use a disciplined life-cycle approach to manage information resources from acquisition through retirement.

4.5. Integrated analysis, planning, budgeting, and evaluation processes shall strengthen the quality of decisions about using IT to meet mission needs. Accordingly:

4.5.1. Performance- and results-based management processes and tools shall guide IT investments and ensure they provide measurable improvements to mission performance. Key steps in implementing these management processes and tools include the following:

4.5.1.1. IRM strategic plans that horizontally and vertically integrate information resources activities throughout the Department, and align IT investments to mission-related outcomes.

4.5.1.2. The Planning, Programming, and Budgeting System (PPBS) and Defense Acquisition System (DAS) processes used as the capital planning and investment control process for maximizing the value and assessing and managing the risks of IT investments.

4.5.1.3 Measurements of performance to gauge progress in achieving IT performance goals.

4.5.1.4. Practices that base decision-making on performance information.

4.5.2. Criteria related to the quantitatively expressed projected net risk-adjusted return on investment and specific quantitative and qualitative criteria shall be used to compare and prioritize alternative IT investment projects.

4.6. Before applying IT:

4.6.1. The DoD Components shall determine whether the functions that IT will support are central to or priorities for the Department's mission. The DoD Strategic Plan, required by reference (l), shall be the bases for identifying:

4.6.1.1. The Department's core mission, priorities, goals, and objectives, and how they will be achieved and measured.

4.6.1.2. What the function contributes to the DoD Strategic Plan and warfighter and customer requirements. The DoD Components shall determine whether the private sector or another Government Agency can perform the particular function more effectively and at less cost.

4.6.2. The DoD Components shall outsource non-core and inherently non-governmental functions to another Government Agency or the private sector when it makes good business sense to do so.

4.6.3. The DoD Components shall routinely and systematically benchmark their functional processes against models of excellence in the public and private sectors. Maximum use shall be made of commercial-off-the-shelf (COTS) and non-developmental item (NDI) products and services when refining, reengineering or redesigning functional processes. Benchmarks and associated analyses, as well as business reengineering practices, methodologies and tools shall be employed by the DoD Components to develop, simplify or refine functional processes before IT solutions are applied.

4.6.4. Information assurance requirements shall be identified by the DoD Components during functional process reengineering, and/or outsourcing.

4.7. Acquisition strategies shall:

4.7.1. Appropriately allocate risk between the Government and a contractor.

4.7.2. Effectively use competition.

4.7.3. Tie contractor payments to performance.

4.7.4. Take maximum advantage of COTS.

4.8. To reduce risks while speeding the delivery of IT capabilities, the DoD Components shall base decisions to develop and modernize IT on the following:

4.8.1. Accurate, detailed descriptions of customer requirements and specifications, and related performance measures that can be used during testing, shall drive the design, development, and support of IT.

4.8.2. Early involvement, buy-in, and feedback from customers/users shall continue throughout the IT project.

4.8.3. Phased, evolutionary IT-acquisition segments that are as brief and narrow in scope as possible. Each segment shall solve a specific part of an overall mission problem and deliver a measurable net benefit independent of future segments.

4.8.4. IT shall be shared and reused wherever possible.

4.8.5. Commercial or non-developmental items shall be used as much as possible, while custom-designed components shall be avoided or isolated to minimize the potential adverse consequences on the overall project.

4.8.6. Initial information system designs shall integrate information assurance components to ensure they provide reliable, timely, and accurate information that is protected, secure, and resilient against information warfare, terrorist, and criminal activities.

4.8.7. Pilots, models, simulations, and prototypes shall be encouraged to gain early insights into required IT capabilities. However, IT capabilities shall be fully tested before going into production.

4.8.8. The DoD Components shall establish and track clear goals (e.g., cost, schedule, and performance), measures, and accountability for IT project progress so that the Component can correct problems quickly as they arise.

4.9. Programs shall be established to acquire, develop and retain a well-trained core of highly qualified IRM and information assurance professionals who can accept, anticipate, and generate the changes that IT will enable.

4.10. Disabled DoD employees or members of the public seeking information or services from the Department of Defense shall have access to and use of information and data comparable to the access and use by individuals who are not disabled, unless an undue burden would be imposed (reference (k)).

5. REPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, as the DoD Chief Information Officer, shall:

5.1.1. Serve as the Principal Staff Assistant for information resources management matters related to references (d) through (i).

5.1.2. Participate in the PPBS process and advise the Secretary and Deputy Secretary of Defense, and the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) on major resource allocation and investment decisions, including recommending whether to continue, modify, or terminate IT investments.

5.1.3. Serve on the Defense Acquisition Board, and advise the USD(AT&L) on IT opportunities and issues related to Defense Acquisition Programs.

5.1.4. Chair the DoD CIO Executive Board (reference (m)), which shall serve as the principal DoD advisory body on matters pertaining to references (d) through (i).

5.1.5. Serve as the DoD primary representative to Federal and interagency bodies supporting Federal IT policies.

5.1.6. Chair the Architecture Coordination Council with the USD(AT&L) and the Joint Community CIO (reference (j)), to

synchronize the Department's architectural activities and establish DoD architectural guidance.

5.1.7. Issue enterprise-wide plans, policies, and procedures that enable the DoD Components to effectively and efficiently manage information resources, including IT, to achieve the Department of Defense's strategic goals.

5.1.8. Promote improvements to DoD work processes and supportive information resources according to reference (i). This shall include developing, maintaining, and issuing guidance on functional process improvement methodologies and their supporting suite of procedures and tools.

5.1.9. Design and implement, with the DoD Planning, Programming, and Budgeting System and Defense Acquisition System authorities, a process for maximizing the value, and assessing and managing the risks of DoD IT acquisitions.

5.1.10. Institutionalize performance- and results-based management for information resources, including IT, in coordination with the DoD Chief Financial Officer (CFO), USD(AT&L), and the DoD Component CIOs.

5.1.11. Monitor and evaluate the performance of Major Automated Information Systems (MAIS) and other DoD IT programs that are of special interest to the Department of Defense, and advise the Secretary and Deputy Secretary of Defense, and USD(AT&L) on whether to continue, modify, or terminate a program.

5.1.12. Develop, maintain, and facilitate, with the Chairman of the Joint Chiefs of Staff and USD(AT&L), the implementation of a sound and integrated IT architecture for IT programs, including NSS, that will increase the value of the Department's information resources.

5.1.13. Establish information assurance policies and procedures that allow the DoD Components to exchange and use information securely meeting both warfighting and business requirements.

5.1.14. Perform the following according to reference (h):

5.1.14.1. Review and provide recommendations to the Secretary and Deputy Secretary of Defense, and USD(AT&L) on DoD budget requests for IT, including NSS.

5.1.14.2. Ensure the interoperability of IT, including NSS, throughout the Department of Defense.

5.1.14.3. Ensure that IT, including NSS, standards that will apply throughout the Department of Defense are prescribed.

5.1.14.4. Institute policies and procedures that provide for the elimination of unnecessarily duplicative IT within the DoD Components and between each other.

5.1.15. Establish policies, programs, and initiatives with the Under Secretary of Defense (Personnel and Readiness) and USD(AT&L) to strengthen DoD personnel's ability to manage information resources effectively.

5.1.16. Implement, monitor, and guide the use of COTS and NDI capabilities, with USD(AT&L), as part of the DoD IT architecture.

5.1.17. Ensure that the IT standards of reference (k) are met.

5.2. The Under Secretary of Defense for Acquisition, Technology and Logistics shall:

5.2.1. Consistent with reference (n), ensure that, where possible, the DoD Acquisition System's process for acquiring IT is simple, clear, and understandable, and specifically addresses managing risk, evolutionary or spiral acquisitions, and incorporating IT in a timely manner.

5.2.2. Chair the Defense Acquisition Board.

5.2.3. Chair the Architecture Coordination Council with the DoD CIO and the Joint Community CIO (reference (j)), to synchronize the Department's architectural activities and establish DoD architectural guidance.

5.2.4. Institutionalize performance- and results-based management for information resources, including IT, in coordination with the DoD CIO, DoD CFO, and the DoD Component CIOs.

5.2.5. Support the development of systems views to develop, maintain, and facilitate the implementation of a sound and integrated IT architecture for IT programs, including NSS, that will increase the value of the Department's information resources in coordination with the Chairman of the Joint Chiefs of Staff and the DoD CIO.

5.2.6. Support and participate in the Chairman of the Joint Chiefs of Staff Requirements Generation System and DoD Component planning to ensure that acquisition reforms and interoperability requirements are visible in warfighting operations and to support seamless transitions between peace and war.

5.3. The Under Secretary of Defense (Comptroller)/Chief Financial Officer shall:

5.3.1. Develop and maintain the DoD Strategic Plan consistent with reference (l).

5.3.2. Establish policies and procedures to ensure that accounting, financial and asset management, and other related DoD IT systems are designed, developed, maintained, and used effectively by the DoD Components to provide financial data reliably, consistently and expeditiously, and support programmatic IT investment decisions.

5.4. The OSD Principal Staff Assistants shall, according to their responsibility and authority for assigned functional areas, including the supporting information systems (ISs):

5.4.1. Improve DoD operations and procedures by ensuring the application of sound business practices, and compliance with this Directive.

5.4.2. Implement, execute, and exercise oversight for the evaluation and improvement of functional processes, as well as the development of functional process performance measures and assessments.

5.4.3. Develop, integrate, implement, and maintain functional strategic plans, objectives, operational and system architectural views, IS strategies, and related models and repository contents that support the functional missions.

5.4.4. Promote commonality and interoperability of functional processes across the DoD Components; resolve functional issues affecting information resources management; and provide resolution for technical ISs integration issues in their functional areas.

5.4.5. Ensure that economic analyses are prepared and validated, as required.

5.4.6. Perform functional management control and oversight of their supporting IS, and ensure functional leadership throughout the systems' life-cycle phases.

5.4.7. Review funding requirements for information resources management and IT programs during planning, programming, and budgeting system activities and recommend appropriate adjustments and allocations.

5.4.8. Perform the following tasks:

5.4.8.1. Designate the DoD-wide automated information systems and applications to support activities and processes that fall within their functional areas.

5.4.8.2. Evolve DoD-wide automated information system and application investments as rapidly as possible for all DoD Components that perform the functional activity.

5.4.8.3. Identify and recommend termination of other automated information systems and applications performing the functional activity.

5.5. The Chairman of the Joint Chiefs of Staff shall:

5.5.1. Appoint a Joint Community CIO, consistent with reference (j).

5.5.2. Improve operations and procedures under his purview by ensuring the application of sound business practices, and compliance with this policy guidance.

5.5.3. Support and participate in functional/business area and DoD Component planning to ensure that the Chairman of the Joint Chiefs of Staff and Commanders-in-Chief requirements for warfighting operations are visible and to support seamless transitions between peace and war.

5.5.4. Validate the linkage of IT support to the joint information requirements of the warfighters.

5.5.5. Perform the following tasks:

5.5.5.1. Designate the joint automated information systems and applications that will be used to support activities and processes that warfighters require.

5.5.5.2. Evolve, with the DoD Components, each joint automated information system and application investment as rapidly as possible for all DoD Components that perform that activity.

5.5.5.3. Identify and recommend termination of other automated information system and application investments performing the activity.

5.6. The Heads of the DoD Components shall:

5.6.1. Appoint the DoD Component CIO who shall have core knowledge, skills, abilities, and experiences to carry out the requirements of reference (d) through (i).

5.6.2. Clearly delineate the DoD Component CIO's IRM role, responsibilities, and authority vis-à-vis those of the DoD Component Comptroller, the Component Acquisition Executive or a similar position, mission/functional area managers, and sub-Component-level CIOs.

5.6.3. Take advantage of the opportunities that IT can provide and ensure that the IT infrastructure will support mission and business strategies by positioning the DoD Component CIO to participate in the Component's long-range strategic planning.

5.6.4. Periodically conduct meetings with the CIO, Comptroller, Component Acquisition Executive or similar position, as well as other key senior managers to promote and forge a strong partnership among them in making strategic Component decisions.

5.6.5. Designate, or authorize the designation of, subordinate-level CIOs as needed.

5.7. The DoD Component Chief Information Officer shall:

5.7.1. Ensure compliance with this Directive and the requirements of references (d) through (i) within the DoD Component.

5.7.2. Provide advice and other assistance to the Component Head and other Component senior management personnel to ensure that information resources are acquired, used, and managed by the DoD Component according to references (d) and (i).

5.7.3. Advise the DoD CIO and implement his or her policies and guidance.

5.7.4. Validate the linkage of Component IT support to the requirements of the warfighters.

5.7.5. Support the selection and implementation of DoD-wide automated information systems and applications in the Component.

5.7.6. Ensure compliance with the standards of reference (k).

6. EFFECTIVE DATE

This Directive is effective immediately.

Enclosures - 2

E1. References, continued

E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

(e) Public Law 104-106, "Division E of the Clinger-Cohen Act of 1996"
(f) Executive Order 13011, "Federal Information Technology," July 16, 1996
(g) Office of Management and Budget Circular A-130, "Management of Federal Information Resources," February 8, 1996
(h) Section 2223 of title 10, United States Code
(i) Secretary of Defense Memorandum, "Implementation of Subdivision E of the Clinger-Cohen Act of 1996 (Public Law 104-106)," June 2, 1997
(j) Chairman of the Joint Chiefs of Staff Instruction 8010.01, "Joint Community Chief Information Officer," July 7, 2000
(k) Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d)
(l) Section 4(b) of Public Law 103-62, 31 U.S.C. 1115, "Government Performance and Results Act of 1993"
(m) DoD Chief Information Officer Executive Board Charter, March 31, 2000
(n) Federal Acquisition Streamlining Act of 1994

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Information. Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

E2.1.2. Information Assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.1.3. Information Life Cycle. The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

E2.1.4. Information Management (IM). The planning, budgeting, manipulating, and controlling of information throughout its life cycle.

E2.1.5. Information Resources. Information and related resources, such as personnel, equipment, funds, and information technology.

E2.1.6. Information Resources Management (IRM). The process of managing information resources to accomplish Agency missions and to improve Agency performance, including through the reduction of information collection burdens on the public.

E2.1.7. Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

E2.1.8. Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD Component directly or is used by a contractor under a contract with the DoD Component that (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

E2.1.9. National Security System (NSS). Any telecommunications or information system operated by the United States Government, the function, operation, or use of which:

E2.1.9.1. Involves intelligence activities.

E2.1.9.2. Involves cryptologic activities related to national security.

E2.1.9.3. Involves command and control of military forces.

E2.1.9.4. Involves equipment that is an integral part of a weapon or weapons system.

E2.1.9.5. Is critical to the direct fulfillment of military or intelligence missions.[14]

[14] This does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Definitions and Acronyms of Commonly Used DoD CIO Terms

ACCB	Architecture and Configuration Control Board
ACTD	Advanced Concept Technology Demonstration
ADR	Annual Defense Report
AIS	automated information system
application	Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs. DoD Directive 8500.1
automated information system application	For DoD information assurance purposes, an automated information system application is the product or deliverable of an acquisition program, such as those described in DoD Directive 5000.1, "The Defense Acquisition System," October 23, 2000. An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense Messaging System). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note that an AIS application is analogous to a "major application" as defined in OMB Circular A-130, "Management of Federal Information Resources, Transmittal 4," November 30, 2000; however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System. DoD Directive 8500.1
BEA	Business Enterprise Architecture
BRM	See Business Reference Model.
Business Reference Model	A function-driven framework used to describe the lines of business and sub-functions performed by the federal government independent of the agencies that perform them. IT investments are mapped to the BRM to identify collaboration opportunities. OMB Circular A-11, Section 53
CAC	common access card
C4	command, control, communications and computers

C4ISR	command, control, communications and computers, intelligence, surveillance and reconnaissance
CCA	Clinger-Cohen Act of 1996
CCB	Configuration Control Board
CES	core enterprise services
chief information officer	The senior official designated by the Secretary of Defense or a Secretary of a military department pursuant to 44 USC 3506. 10 USC 2223
CIM	common information model; corporate information management
CIO	See chief information officer; also, chief information office.
CM	configuration management
CND	computer network defense
COE	common operating environment
Computer network	The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities such as local or campus area networks, or long-haul data transport capabilities such as operational, metropolitan, or wide area and backbone networks. DoD Directive 8500.1
computing environment	Workstation or server (host) and its operating system, peripherals, and applications. DoD Directive 8500.1
COI	community of interest
CONOPS	contingency operations; concept of operations
COOP	continuity of operations
COP	community of practice; common operational picture
COTS	commercial off the shelf
DAB	Defense Acquisition Board
Data Reference Model	A framework used to promote the common identification, use, and appropriate sharing of data/information across the federal government. It provides standards and guidelines to help agencies structure, categorize, exchange, and manage their data to improve the ability of government to perform cross-agency information sharing. OMB Circular A-11, Section 53
DCIO	Deputy Chief Information Officer
DDMS	DoD Discovery Metadata System
Defense Information Systems Network	The DoD consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. DoD Directive 8500.1

Defense-in-Depth	The DoD approach for establishing an adequate information assurance posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA solutions within and among IT assets; and, the selection of IA solutions based on their relative level of robustness. DoD Directive 8500.1
Demilitarized Zone	Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's IA policy for external information exchanges and to provide external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks. A DMZ is also called a "screened subnet." DoD Directive 8500.1
DIA	Defense Intelligence Agency
DIACAP	Defense Information Assurance Certification and Accreditation Program
DIAP	Defense-wide Information Assurance Program
DISA	Defense Information Systems Agency
DISN	See Defense Information Systems Network.
DISR	Defense Information Technology Standards Registry
DITPR	DoD Information Technology Portfolio Repository
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMZ	See Demilitarized Zone.
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DPG	Defense Planning Guidance
DRB	Defense Resources Board
DRM	See Data Reference Model.
DSAWG	DISN Security Accreditation Working Group
DSN	Defense Switched Network
EA	See enterprise architecture; executive agent.
e-gov	See electronic government.
EIE	See enterprise information environment.
EIEMA	Enterprise Information Environment Mission Area
Electronic Government	The use by the government of web-based Internet applications and other information technologies, combined with processes that implement these technologies, to (A) enhance the access to and delivery of government information and services to the public, other agencies, and other government entities; or (B) bring about improvements in govern-

	ment operations that may include effectiveness, efficiency, service quality, or transformation. E-Government Act
enterprise architecture	A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan. E-Government Act
enterprise information environment	The common, integrated information computing and communications environment of the Global Information Grid (GIG). The EIE is composed of GIG assets that operate as, provide transport for and/or assure local area networks, campus area networks, tactical operational and strategic networks, metropolitan area networks, and wide area networks. The EIE includes computing infrastructure for the automatic acquisition, storage, manipulation, management, control, and display of data or information, with a primary emphasis on DoD enterprise hardware, software operating systems, and hardware/software support that enable the GIG enterprise. The EIE also includes a common set of enterprise services, called Core Enterprise Services, which provide awareness of, access to, and delivery of information on the GIG. DoD Directive 8115.01
ES	enterprise services
ESI	Enterprise Software Initiative
FEA	See Federal Enterprise Architecture.
FCIOC	Federal Chief Information Officers Council
Federal Enterprise Architecture	A business-based framework for government-wide improvement. It describes the relationship between business functions and the technologies and information that support them. The FEA is being constructed through a collection of interrelated "reference models" designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across federal agencies. OMB Circular A-11, Section 53
FISMA	Federal Information Security Management Act
FTS	Federal Telecommunications System
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GIG	See Global Information Grid.
GIG-BE	Global Information Grid – Bandwidth Expansion
GIG-ES	Global Information Grid – Enterprise Service
GISRA	Government Information Security Reporting Act

Global Information Grid	The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996 (reference (b)). The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. It includes any system, equipment, software, or service that meets one or more of the following criteria a) Transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services; b) Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services; c) Processes data or information for use by other equipment, software, or services. Non-GIG IT – Stand-alone, self-contained, or embedded IT that is not and will not be connected to the enterprise network. DoD Directive 8100.1
GPEA	Government Paperwork Elimination Act
GPRA	Government Performance and Results Act
HAIPE	High Assurance Internet Protocol Encryption
HF	Horizontal Fusion
IA	See information assurance.
IASLG	Information Assurance Senior Leadership Group
IAVA	information assurance vulnerability alert
IC	Intelligence Community
information	Any communication or representation of knowledge such as facts, data, or opinion in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. DoD Directive 8001.1
information assurance	Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. DoD Directive 8000.1

Information Assurance Certification and Accreditation	The standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD information systems. DoD Directive 8500.1
information management	The planning, budgeting, manipulating, and controlling of information throughout its life cycle. DoD Directive 8001.1
information owner	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. DoD Directive 8500.1
information resources	Information and related resources, such as personnel, equipment, funds, and information technology. 44 USC 3502
information resources management	The process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of information collection burdens on the public. 44 USC 3502(7)
information security	Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; (C) availability, which means ensuring timely and reliable access to and use of information; and (D) authentication, which means utilizing digital credentials to assure the identity of users and validate their access. 44 USC 3532(b)(1)
Information Superiority	The capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. DoD Directive 8100.1
information system	Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, and includes (A) computers and computer networks; (B) ancillary equipment; (C) software, firmware, and related procedures; (D) services, including support services; and (E) related resources. 44 USC 3532
information system life cycle	The phases through which an information system passes, typically characterized as initiation, development, operation, and termination. OMB Circular A-130
information technology	(A) Any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, trans-

	mission, or reception of data or information by the executive agency, if the equip-ment is used by the executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; (B) includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources; but (C) does not include any equipment acquired by a federal contractor incidental to a federal contract. 40 USC 11101
information technology architecture	An integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals. 40 USC 11315
information technology investment	The development and sustainment resources needed in support of IT or IT-related initiatives. These resources include, but are not limited to: research, development, test, and evaluation appropriations; procurement appropriations; military personnel appropriations; operations and maintenance appropriations; and Defense Working Capital Fund. DoD Directive 8115.01
information technology portfolio	A grouping of information technology investments by capability to accomplish a specific functional goal, objective, or mission outcome. DoD Directive 8115.01
information technology portfolio management	The management of selected groupings of information technology investments using strategic planning, architectures, and outcome-based performance measures to achieve a mission capability. DoD Directive 8115.01
information technology not a part of GIG	Generally, stand-alone, self-contained, or embedded information technology that is not and shall not be connected to the enterprise network. DoD Directive 8115.01
IOC	initial operating capability
IOT&E	initial operational test and evaluation
IPv6	Internet Protocol Version 6
IRB	investment review board
IRM	information resources management
IRMC	Information Resources Management College
IS	See information security; information system.
ISOP	Information Technology Standards Oversight Panel
ISRP	Interoperability Senior Review Panel
ISWG	Information Technology Standards Working Group

IT-CoP	See information technology community of practice.
ITMRA	Information Technology Management Reform Act
ITSC	Information Technology Standards Committee
JCIDS	Joint Capabilities Integration and Development System
JFCOM	U.S. Joint Forces Command
JPG	Joint Programming Guidance
JROC	Joint Requirements Oversight Council
JTA	Joint Technical Architecture
JTF-GNO	Joint Task Force – Global Network Operations
JWICS	Joint Worldwide Intelligence Communications System
MAC, MAC I, MAC II, MAC III	See mission assurance category, I, II and III.
MAIS	major automated information system
Major system	A combination of elements that will function together to produce the capabilities required to fulfill a mission need, which elements may include hardware, equipment, software or any combination thereof, but excludes construction or other improvements to real property. A system shall be considered a major system if (i) the Department of Defense is responsible for the system and the total expenditures for research, development, test and evaluation for the system are estimated to be more than $75,000,000 (based on fiscal year 1980 constant dollars) or the eventual total expenditure for procurement of more than $300,000,000 (based on fiscal year 1980 constant dollars); (ii) a civilian agency is responsible for the system and total expenditures for the system are estimated to exceed $750,000 (based on fiscal year 1980 constant dollars) or the dollar threshold for a "major system" established by the agency pursuant to Office of Management and Budget (OMB) Circular A–109, entitled "Major Systems Acquisitions", whichever is greater; or (iii) the system is designated a "major system" by the head of the agency responsible for the system. 41 USC 43(9)
MCEB	Military Communications-Electronics Board
Mission area	A defined area of responsibility with functions and processes that contribute to mission accomplishment. DoD Directive 8115.01
Mission Assurance Category	Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. DoD has three defined mission assurance categories. DoD Directive 8500.1

Mission Assurance Category I	Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures. DoD Directive 8500.1
Mission Assurance Category II	Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance. DoD Directive 8500.1
Mission Assurance Category III	Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices. DoD Directive 8500.1
MNIS	multi-national information sharing
National Security System	(A) Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which (I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons system; or (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (B) Subparagraph (i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). 44 USC 3542
NC	net-centricity; net-centric
NCES	Net-Centric Enterprise Services

NCOW	Net-Centric Operations and Warfare
NCW	Net-Centric Warfare
NDU	National Defense University
NetOps	net-centric operations; network operations
NII	Networks and Information Integration
NIPRNet	Non-Secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NMCI	Navy-Marine Corps Intranet
NOC	Network Operation Center
NOSC	Network Operations and Security Center
NSS	See National Security System.
OHIO	Only handle information once
OIRA	Office of Information and Regulatory Affairs
PIA	Privacy Impact Assessment
PKI	public key infrastructure
PPBE	Planning, Programming, Budgeting and Execution
PRM	Performance Reference Model
QDR	Quadrennial Defense Review
records	Includes all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included. 44 USC 3301
records management	The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. 44 U.S.C. 2901(2)
SAM	software asset management
SBU	sensitive but unclassified

SE	systems engineering
SCI	sensitive compartmented information
SIPRNet	Secure Internet Protocol Router Network
SPG	Strategic Planning Guidance
STRATCOM	U.S. Strategic Command
Technical Reference Model	A foundation used to describe the standards, specifications, and technologies supporting the delivery, exchange, and construction of business (or service) components and E-Gov solutions. The TRM unifies existing agency TRMs and E-Gov guidance by providing a foundation to advance the re-use of technology and component services from a government-wide perspective. OMB Circular A-11
TRM	See Technical Reference Model.
UCP	Unified Command Plan

Table of Contents - Volume II, Supplemental Materials