107TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPT. 107–787
Part 1

E-GOVERNMENT ACT OF 2002

NOVEMBER 14, 2002.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. BURTON of Indiana, from the Committee on Government Reform, submitted the following

R E P O R T

[To accompany H.R. 2458]

[Including cost estimate of the Congressional Budget Office]

The Committee on Government Reform, to whom was referred the bill (H.R. 2458) to enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 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:

SEC. 2. FINDINGS AND PURPOSES.

(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.

TITLE I—OFFICE OF MANAGEMENT AND BUDGET ELECTRONIC GOVERNMENT SERVICES

SEC. 101. MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES.

(a) IN GENERAL.—Title 44, United States Code, is amended by inserting after chapter 35 the following:

"CHAPTER 36—MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

"§ 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 the governing body of any Indian tribe, band, nation, or other organized group or community, including any Alaska Native village or regional or village corporation as defined in or established pursuant to the Alaska Native Claims Settlement Act (43 U.S.C. 1601 et seq.), which is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians.

"§ 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 under section 11331 of title 40, to be developed by the National Institute of Standards and Technology and promulgated by the Secretary of Commerce, 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.

"§ 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 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.

"(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.

"§ 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.

"§ 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.

"§ 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.".

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of chapters for title 44, United States Code, is amended by inserting after the item relating to chapter 35 the following:

"36. Management and Promotion of Electronic Government Services ..... 3601".

SEC. 102. CONFORMING AMENDMENTS.

(a) ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGIES.—

(1) IN GENERAL.—Chapter 3 of title 40, United States Code, is amended by inserting after section 304 the following new section:

"§ 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.".

(2) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 3 of such title is amended by inserting after the item relating to section 304 the following:

"305. Electronic Government and information technologies.".

(b) MODIFICATION OF DEPUTY DIRECTOR FOR MANAGEMENT FUNCTIONS.—Section 503(b) of title 31, United States Code, is amended—

(1) by redesignating paragraphs (5), (6), (7), (8), and (9), as paragraphs (6), (7), (8), (9), and (10), respectively; and

(2) by inserting after paragraph (4) the following:

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

(c) OFFICE OF ELECTRONIC GOVERNMENT.—

(1) IN GENERAL.—Chapter 5 of title 31, United States Code, is amended by inserting after section 506 the following:

"§ 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.".

(2) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 5 of title 31, United States Code, is amended by inserting after the item relating to section 506 the following:

"507. Office of Electronic Government.".

TITLE II—FEDERAL MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

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 (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 information technology standards promulgated under this Act 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 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 under this Act 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; 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 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), 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. 205. FEDERAL COURTS.

(a) INDIVIDUAL COURT WEBSITES.—The Chief Justice of the United States, the chief judge of each circuit and district, and the chief bankruptcy judge of each district shall establish with respect to the Supreme Court or the respective court of appeals, district, or bankruptcy court of a district, a website that contains the following information or links to websites with the following information:

(1) Location and contact information for the courthouse, including the telephone numbers and contact names for the clerk's office and justices' or judges' chambers.

(2) Local rules and standing or general orders of the court.

(3) Individual rules, if in existence, of each justice or judge in that court.

(4) Access to docket information for each case.

(5) Access to the substance of all written opinions issued by the court, regardless of whether such opinions are to be published in the official court reporter, in a text searchable format.

(6) Access to all documents filed with the courthouse in electronic form, described under subsection (c).

(7) Any other information (including forms in a format that can be downloaded) that the court determines useful to the public.

(b) MAINTENANCE OF DATA ONLINE.—

(1) UPDATE OF INFORMATION.—The information and rules on each website shall be updated regularly and kept reasonably current.

(2) CLOSED CASES.—Electronic files and docket information for cases closed for more than 1 year are not required to be made available online, except all written opinions with a date of issuance after the effective date of this section shall remain available online.

(c) ELECTRONIC FILINGS.—

(1) IN GENERAL.—Except as provided under paragraph (2), each court shall make any document that is filed electronically publicly available online. A court may convert any document that is filed in paper form to electronic form. To the extent such conversions are made, all such electronic versions of the document shall be made available online.

(2) EXCEPTIONS.—Documents that are filed that are not otherwise available to the public, such as documents filed under seal, shall not be made available online.

(3) PRIVACY AND SECURITY CONCERNS.—The Judicial Conference of the United States may promulgate rules under this subsection to protect important privacy and security concerns.

(d) DOCKETS WITH LINKS TO DOCUMENTS.—The Judicial Conference of the United States shall explore the feasibility of technology to post online dockets with links allowing all filings, decisions, and rulings in each case to be obtained from the docket sheet of that case.

(e) COST OF PROVIDING ELECTRONIC DOCKETING INFORMATION.—Section 303(a) of the Judiciary Appropriations Act, 1992 (28 U.S.C. 1913 note) is amended in the first sentence by striking "shall hereafter" and inserting "may, only to the extent necessary,".

(f) TIME REQUIREMENTS.—Not later than 2 years after the effective date of this title, the websites under subsection (a) shall be established, except that access to documents filed in electronic form shall be established not later than 4 years after that effective date.

(g) DEFERRAL.—

(1) IN GENERAL.—

(A) ELECTION.—

(i) NOTIFICATION.—The Chief Justice of the United States, a chief judge, or chief bankruptcy judge may submit a notification to the Administrative Office of the United States Courts to defer compliance with any requirement of this section with respect to the Supreme Court, a court of appeals, district, or the bankruptcy court of a district.

(ii) CONTENTS.—A notification submitted under this subparagraph shall state—

(I) the reasons for the deferral; and

(II) the online methods, if any, or any alternative methods, such court or district is using to provide greater public access to information.

(B) EXCEPTION.—To the extent that the Supreme Court, a court of appeals, district, or bankruptcy court of a district maintains a website under subsection (a), the Supreme Court or that court of appeals or district shall comply with subsection (b)(1).

(2) REPORT.—Not later than 1 year after the effective date of this title, and every year thereafter, the Judicial Conference of the United States shall submit a report to the Committees on Governmental Affairs and the Judiciary of the Senate and the Committees on Government Reform and the Judiciary of the House of Representatives that—

(A) contains all notifications submitted to the Administrative Office of the United States Courts under this subsection; and

(B) summarizes and evaluates all notifications.

SEC. 206. REGULATORY AGENCIES.

(a) PURPOSES.—The purposes of this section are to—

(1) improve performance in the development and issuance of agency regulations by using information technology to increase access, accountability, and transparency; and

(2) enhance public participation in Government by electronic means, consistent with requirements under subchapter II of chapter 5 of title 5, United States Code, (commonly referred to as the "Administrative Procedures Act").

(b) INFORMATION PROVIDED BY AGENCIES ONLINE.—To the extent practicable as determined by the agency in consultation with the Director, each agency (as defined under section 551 of title 5, United States Code) shall ensure that a publicly accessible Federal Government website includes all information about that agency required to be published in the Federal Register under paragraphs (1) and (2) of section 552(a) of title 5, United States Code.

(c) SUBMISSIONS BY ELECTRONIC MEANS.—To the extent practicable, agencies shall accept submissions under section 553(c) of title 5, United States Code, by electronic means.

(d) ELECTRONIC DOCKETING.—

(1) IN GENERAL.—To the extent practicable, as determined by the agency in consultation with the Director, agencies shall ensure that a publicly accessible Federal Government website contains electronic dockets for rulemakings under section 553 of title 5, United States Code.

(2) INFORMATION AVAILABLE.—Agency electronic dockets shall make publicly available online to the extent practicable, as determined by the agency in consultation with the Director—

(A) all submissions under section 553(c) of title 5, United States Code; and

(B) other materials that by agency rule or practice are included in the rulemaking docket under section 553(c) of title 5, United States Code, whether or not submitted electronically.

(e) TIME LIMITATION.—Agencies shall implement the requirements of this section consistent with a timetable established by the Director and reported to Congress in the first annual report under section 3606 of title 44 (as added by this Act).

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, 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, 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

(iii) 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 standards promulgated by the Secretary of Commerce 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, 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, 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, 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, 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, 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, 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 Government-wide 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 developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form.

(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, 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) 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

(C) assess the training of Federal employees in information technology disciplines, as necessary, in order to ensure that the information resource management needs of the Federal Government are addressed.

(2) AUTHORITY TO DETAIL EMPLOYEES TO NON-FEDERAL EMPLOYERS.—In carrying out paragraph (1), 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.

(3) COORDINATION PROVISION.—An assignment described in section 3703 of title 5, United States Code, shall be made only in accordance with the program established under paragraph (2), if any.

(4) 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, agen-

cies shall encourage employees to participate in occupational information technology training.

(5) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Office of Personnel Management for the implementation of this subsection, $7,000,000 in fiscal year 2003, and such sums as are necessary for each fiscal year thereafter.

(c) INFORMATION TECHNOLOGY EXCHANGE PROGRAM.—

(1) IN GENERAL.—Subpart B of part III of title 5, United States Code, is amended by adding at the end the following:

"CHAPTER 37—INFORMATION TECHNOLOGY EXCHANGE PROGRAM

"§ 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.

"§ 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.

"§ 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.".

(2) REPORT.—Not later than 4 years after the date of the enactment of this Act, 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.—The analysis for part III of title 5, United States Code, is amended by inserting after the item relating to chapter 35 the following:

"37. Information Technology Exchange Program ..... 3701".

(d) ETHICS PROVISIONS.—

(1) ONE-YEAR RESTRICTION ON CERTAIN COMMUNICATIONS.—Section 207(c)(2)(A) of title 18, United States Code, is amended—

(A) by striking "or" at the end of clause (iii);

(B) by striking the period at the end of clause (iv) and inserting "; or"; and

(C) by adding at the end the following:

"(v) assigned from a private sector organization to an agency under chapter 37 of title 5.".

(2) DISCLOSURE OF CONFIDENTIAL INFORMATION.—Section 1905 of title 18, United States Code, is amended by inserting "or being an employee of a private sector organization who is or was assigned to an agency under chapter 37 of title 5," after "(15 U.S.C. 1311–1314),".

(3) CONTRACT ADVICE.—Section 207 of title 18, United States Code, is amended by adding at the end the following:

"(l) CONTRACT ADVICE BY FORMER DETAILS.—Whoever, being an employee of a private sector organization assigned to an agency under chapter 37 of title 5, within one year after the end of that assignment, knowingly represents or aids, counsels, or assists in representing any other person (except the United States) in connection with any contract with that agency shall be punished as provided in section 216 of this title.".

(4) RESTRICTION ON DISCLOSURE OF PROCUREMENT INFORMATION.—Section 27 of the Office of Federal Procurement Policy Act (41 U.S.C. 423) is amended in subsection (a)(1) by adding at the end the following new sentence: "In the case of an employee of a private sector organization assigned to an agency under chapter 37 of title 5, United States Code, in addition to the restriction in the preceding sentence, such employee shall not, other than as provided by law, knowingly disclose contractor bid or proposal information or source selection information during the three-year period after the end of the assignment of such employee.".

(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, 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.—Title 5, United States Code, is amended—

(A) in section 3111, by adding at the end the following:

"(d) Notwithstanding section 1342 of title 31, the head of an agency may accept voluntary service for the United States under chapter 37 of this title and regulations of the Office of Personnel Management.";

(B) in section 4108, by striking subsection (d); and

(C) in section 7353(b), by adding at the end the following:

"(4) Nothing in this section precludes an employee of a private sector organization, while assigned to an agency under chapter 37, from continuing to receive pay and benefits from such organization in accordance with such chapter.".

(2) AMENDMENT TO TITLE 18, UNITED STATES CODE.—Section 209 of title 18, United States Code, is amended by adding at the end the following:

"(g)(1) This section does not prohibit an employee of a private sector organization, while assigned to an agency under chapter 37 of title 5, from continuing to receive pay and benefits from such organization in accordance with such chapter.

"(2) For purposes of this subsection, the term 'agency' means an agency (as defined by section 3701 of title 5) and the Office of the Chief Technology Officer of the District of Columbia.".

(3) OTHER AMENDMENTS.—Section 125(c)(1) of Public Law 100–238 (5 U.S.C. 8432 note) is amended—

(A) in subparagraph (B), by striking "or" at the end;

(B) in subparagraph (C), by striking "and" at the end and inserting "or"; and

(C) by adding at the end the following:

"(D) an individual assigned from a Federal agency to a private sector organization under chapter 37 of title 5, United States Code; and".

SEC. 210. SHARE-IN-SAVINGS INITIATIVES.

(a) DEFENSE CONTRACTS.—(1) Chapter 137 of title 10, United States Code, is amended by adding at the end the following new section:

"§ 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. 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—

"(i) may not exceed 5, in each of fiscal years 2003, 2004, and 2005; and

"(ii) may not exceed 10, in each of fiscal years 2006, 2007, 2008, and 2009.

"(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.

"(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, 2009.".

(2) The table of sections at the beginning of such chapter is amended by adding at the end of the following new item:

"2332. Share-in-savings contracts.".

(b) OTHER CONTRACTS.—Title III of the Federal Property and Administrative Services Act of 1949 is amended by adding at the end the following:

"SEC. 317. 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, United States Code) 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. 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 chapter applies in a fiscal year—

"(i) may not exceed 5, in each of fiscal years 2003, 2004, and 2005; and

"(ii) may not exceed 10, in each of fiscal years 2006, 2007, 2008, and 2009.

"(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.

"(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, 2009.".

(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, 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, 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 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; and

(2) any recommendations, as the Comptroller General deems appropriate, on the use of share-in-savings contracts by executive agencies.

(h) 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 (as added by subsection (b)).

SEC. 211. AUTHORIZATION FOR ACQUISITION OF INFORMATION TECHNOLOGY BY STATE AND LOCAL GOVERNMENTS THROUGH FEDERAL SUPPLY SCHEDULES.

(a) AUTHORITY TO USE CERTAIN SUPPLY SCHEDULES.—Section 502 of title 40, United States Code, is amended by adding at the end the following new subsection:

"(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 a tribal organization, as defined in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

"(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)).".

(b) PROCEDURES.—Not later than 30 days after the date of the enactment of this Act, the Administrator of General Services shall establish procedures to implement section 501(c) of title 40, United States Code (as added by subsection (a)).

(c) REPORT.—Not later than December 31, 2004, the Administrator shall 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 implementation and effects of the amendment made by subsection (a).

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, 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. 213. COMMUNITY TECHNOLOGY CENTERS.

(a) PURPOSES.—The purposes of this section are to—

(1) study and enhance the effectiveness of community technology centers, public libraries, and other institutions that provide computer and Internet access to the public; and

(2) promote awareness of the availability of on-line government information and services, to users of community technology centers, public libraries, and other public facilities that provide access to computer technology and Internet access to the public.

(b) STUDY AND REPORT.—Not later than 2 years after the effective date of this title, the Administrator shall—

(1) conduct a study to evaluate the best practices of community technology centers that have received Federal funds; and

(2) submit a report on the study to—

(A) the Committee on Governmental Affairs of the Senate;

(B) the Committee on Health, Education, Labor, and Pensions of the Senate;

(C) the Committee on Government Reform of the House of Representatives; and

(D) the Committee on Education and the Workforce of the House of Representatives.

(c) CONTENTS.—The report under subsection (b) may consider—

(1) an evaluation of the best practices being used by successful community technology centers;

(2) a strategy for—

(A) continuing the evaluation of best practices used by community technology centers; and

(B) establishing a network to share information and resources as community technology centers evolve;

(3) the identification of methods to expand the use of best practices to assist community technology centers, public libraries, and other institutions that provide computer and Internet access to the public;

(4) a database of all community technology centers that have received Federal funds, including—

(A) each center's name, location, services provided, director, other points of contact, number of individuals served; and

(B) other relevant information;

(5) an analysis of whether community technology centers have been deployed effectively in urban and rural areas throughout the Nation; and

(6) recommendations of how to—

(A) enhance the development of community technology centers; and

(B) establish a network to share information and resources.

(d) COOPERATION.—All agencies that fund community technology centers shall provide to the Administrator any information and assistance necessary for the completion of the study and the report under this section.

(e) ASSISTANCE.—

(1) IN GENERAL.—The Administrator, in consultation with the Secretary of Education, shall work with other relevant Federal agencies, and other interested persons in the private and nonprofit sectors to—

(A) assist in the implementation of recommendations; and

(B) identify other ways to assist community technology centers, public libraries, and other institutions that provide computer and Internet access to the public.

(2) TYPES OF ASSISTANCE.—Assistance under this subsection may include—

(A) contribution of funds;

(B) donations of equipment, and training in the use and maintenance of the equipment; and

(C) the provision of basic instruction or training material in computer skills and Internet usage.

(f) ONLINE TUTORIAL.—

(1) IN GENERAL.—The Administrator, in consultation with the Secretary of Education, the Director of the Institute of Museum and Library Services, other relevant agencies, and the public, shall develop an online tutorial that—

(A) explains how to access Government information and services on the Internet; and

(B) provides a guide to available online resources.

(2) DISTRIBUTION.—The Administrator, with assistance from the Secretary of Education, shall distribute information on the tutorial to community technology centers, public libraries, and other institutions that afford Internet access to the public.

(g) PROMOTION OF COMMUNITY TECHNOLOGY CENTERS.—The Administrator, with assistance from the Department of Education and in consultation with other agencies and organizations, shall promote the availability of community technology centers to raise awareness within each community where such a center is located.

(h) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for the study of best practices at community technology centers, for the development and dissemination of the online tutorial, and for the promotion of community technology centers under this section—

(1) $2,000,000 in fiscal year 2003;

(2) $2,000,000 in fiscal year 2004; and

(3) such sums as are necessary in fiscal years 2005 through 2007.

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, the Administrator, in consultation with the Federal Emergency Management Agency, shall enter into a contract to conduct a study 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. 215. DISPARITIES IN ACCESS TO THE INTERNET.

(a) STUDY AND REPORT.—

(1) STUDY.—Not later than 90 days after the date of enactment of this Act, the Administrator of General Services shall request that the National Academy of Sciences, acting through the National Research Council, enter into a contract to conduct a study on disparities in Internet access for online Government services.

(2) REPORT.—Not later than 2 years after the date of enactment of this Act, the Administrator of General Services shall submit to the Committee on Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives a final report of the study under this section, which shall set forth the findings, conclusions, and recommendations of the National Research Council.

(b) CONTENTS.—The report under subsection (a) shall include a study of—

(1) how disparities in Internet access influence the effectiveness of online Government services, including a review of—

(A) the nature of disparities in Internet access;

(B) the affordability of Internet service;

(C) the incidence of disparities among different groups within the population; and

(D) changes in the nature of personal and public Internet access that may alleviate or aggravate effective access to online Government services;

(2) how the increase in online Government services is influencing the disparities in Internet access and how technology development or diffusion trends may offset such adverse influences; and

(3) related societal effects arising from the interplay of disparities in Internet access and the increase in online Government services.

(c) RECOMMENDATIONS.—The report shall include recommendations on actions to ensure that online Government initiatives shall not have the unintended result of increasing any deficiency in public access to Government services.

(d) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated $950,000 in fiscal year 2003 to carry out this section.

TITLE III—INFORMATION SECURITY

SEC. 301. INFORMATION SECURITY.

(a) SHORT TITLE.—This title may be cited as the "Federal Information Security Management Act of 2002".

(b) INFORMATION SECURITY.—

(1) IN GENERAL.—Subchapter II of chapter 35 of title 44, United States Code, is amended to read as follows:

"SUBCHAPTER II—INFORMATION SECURITY

"§ 3531. 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.

"§ 3532. 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 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; and

"(C) availability, which means ensuring timely and reliable access to and use of information;

"(2) 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—

"(A) 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) is critical to the direct fulfillment of military or intelligence missions,

except that this subparagraph does not include a system that is used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or

"(B) 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; and

"(3) the term 'information technology' has the meaning given that term in section 11101 of title 40.

"§ 3533. Authority and functions of the Director

"(a) 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 the promulgation of standards and guidelines 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 3534(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 3536; 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 3535;

"(B) significant deficiencies in agency information security practices;

"(C) planned remedial action to address such deficiencies; and

"(D) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section

20(e)(7) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

"(b) 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.

"§ 3534. Federal agency responsibilities

"(a) 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 by the Director 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 3533 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) Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3533(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 evaluation under section 3535;

"(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 3536(b), including—

"(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 3536; 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) 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 of this chapter;

"(C) information technology management under subtitle III of title 40;

"(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, (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)(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) Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

"§ 3535. Annual independent evaluation

"(a)(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 by an agency 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) Subject to subsection (c)—

"(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978, 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) 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) 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)(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 con-

tain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

"(f) 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)(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3533(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) 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.

"§ 3536. Federal information security incident center

"(a) 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 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) 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.

"§ 3537. 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.

"§ 3538. 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.

"§ 3539. Effect on existing law

"Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards 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 informa-

tion resources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States.".

(2) CLERICAL AMENDMENT.—The items in the table of sections at the beginning of such chapter 35 under the heading "SUBCHAPTER II—INFORMATION SECURITY" are amended to read as follows:

"3531. Purposes.
"3532. Definitions.
"3533. Authority and functions of the Director.
"3534. Federal agency responsibilities.
"3535. Annual independent evaluation.
"3536. Federal information security incident center.
"3537. National security systems.
"3538. Authorization of appropriations.
"3539. Effect on existing law.".

(c) INFORMATION SECURITY RESPONSIBILITIES OF CERTAIN AGENCIES.—

(1) NATIONAL SECURITY RESPONSIBILITIES.—(A) Nothing in this Act (including any amendment made by this Act) shall supersede any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems, as defined by section 3532(b)(2) of title 44, United States Code.

(B) Section 2224 of title 10, United States Code, is amended—

(i) in subsection (b), by striking "(b) OBJECTIVES AND MINIMUM REQUIREMENTS.—(1)" and inserting "(b) OBJECTIVES OF THE PROGRAM.—";

(ii) in subsection (b), by striking paragraph (2); and

(iii) in subsection (c), in the matter preceding paragraph (1), by inserting ", including through compliance with subtitle II of chapter 35 of title 44" after "infrastructure".

(2) ATOMIC ENERGY ACT OF 1954.—Nothing in this Act shall supersede any requirement made by or under the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.). Restricted data or formerly restricted data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).

SEC. 302. MANAGEMENT OF INFORMATION TECHNOLOGY.

(a) IN GENERAL.—Section 11331 of title 40, United States Code, is amended to read as follows:

"§ 11331. Responsibilities for federal information systems standards

"(a) INFORMATION SECURITY STANDARDS.—

"(1) IN GENERAL.—(A) 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 paragraph (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)), promulgate information security standards pertaining to Federal information systems.

"(B) 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) Information security standards described under subparagraph (B) shall be compulsory and binding.

"(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems under this subsection shall be developed, promulgated, enforced, and overseen as otherwise authorized by law and as directed by the President.

"(3) AGENCY HEAD AUTHORITY.—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 subsection, if such standards—

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

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

"(4) DECISIONS ON PROMULGATION OF STANDARDS.—(A) The decision regarding the promulgation of any standard by the Director under paragraphs (1) and (2) 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).

"(B) 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.

"(b) ADDITIONAL STANDARDS RELATING TO FEDERAL INFORMATION SYSTEMS.—

"(1) IN GENERAL.—Except as provided under paragraph (2), the Secretary of Commerce shall, on the basis of proposed standards developed by the National Institute of Standards and Technology pursuant to paragraph (2) 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 Director of the Office of Management and Budget, promulgate standards pertaining to Federal information systems. The Secretary shall make such standards compulsory and binding to the extent that the Secretary determines necessary to improve the efficiency and effectiveness of the operation of Federal information systems.

"(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems under this subsection shall be developed, promulgated, enforced, and overseen as otherwise authorized by law and as directed by the President.

"(3) AUTHORITY OF SECRETARY.—The authority conferred upon the Secretary of Commerce by this subsection shall be exercised subject to direction by the President and in coordination with the Director of the Office of Management and Budget to ensure fiscal and policy consistency.

"(4) AGENCY HEAD AUTHORITY.—The head of an agency may employ standards for information systems that are more stringent than the standards promulgated by the Secretary of Commerce under this subsection, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

"(c) DEFINITIONS.—In this section:

"(1) FEDERAL INFORMATION SYSTEM.—The term 'Federal information system' means an information system used or operated by an agency, by a contractor of an agency, or by another organization on behalf of an agency.

"(2) INFORMATION SECURITY.—The term 'information security' has the meaning given that term in section 3532(b)(1) of title 44.

"(3) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given that term in section 3532(b)(2) of title 44.".

(b) CLERICAL AMENDMENT.—The item relating to section 11331 in the table of sections at the beginning of chapter 113 of such title is amended to read as follows:

"11331. Responsibilities for Federal information systems standards.".

SEC. 303. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.

Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), is amended by striking the text and inserting the following:

"(a) 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, United States Code); and

"(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.

"(b) The standards and guidelines required by subsection (a) 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) In developing standards and guidelines required by subsections (a) and (b), the Institute shall—

"(1) consult with other agencies and offices and the private sector (including 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, United States Code—

"(A) standards, as required under subsection (b)(1)(A), no later than 12 months after the date of the enactment of this section; and

"(B) minimum information security requirements for each category, as required under subsection (b)(1)(C), no later than 36 months after the date of the enactment of this section;

"(4) issue guidelines as required under subsection (b)(1)(B), no later than 18 months after the date of the enactment of this section;

"(5) ensure that such standards and guidelines do not specify the use or procurement of certain products, including any specific hardware or software;

"(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)(1) There is established in the Institute an Office for Information Security Programs.

"(2) The Office for Information Security Programs shall be headed by a Director, who shall be a senior executive and shall be compensated at a level in the Senior Executive Service under section 5382 of title 5, United States Code, as determined by the Secretary of Commerce.

"(3) The Director of the Institute shall delegate to the Director of the Office of Information Security Programs the authority to administer all functions under this section, except that any such delegation shall not relieve the Director of the Institute of responsibility for the administration of such functions. The Director of the Office of Information Security Programs shall serve as principal adviser to the Director of the Institute on all functions under this section.

"(e) The Institute shall—

"(1) submit standards developed pursuant to subsection (a), 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, United States Code;

"(2) provide assistance to agencies regarding—

"(A) compliance with the standards and guidelines developed under subsection (a);

"(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 21, regarding standards and guidelines developed under subsection (a) 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.

"(f) As used in this section—

"(1) the term 'agency' has the same meaning as provided in section 3502(1) of title 44, United States Code;

"(2) the term 'information security' has the same meaning as provided in section 3532(b)(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, United States Code; and

"(5) the term 'national security system' has the same meaning as provided in section 3532(b)(2) of title 44, United States Code.

"(g) There are authorized to be appropriated to the Secretary of Commerce $20,000,000 for each of fiscal years 2003, 2004, 2005, 2006, and 2007 to enable the National Institute of Standards and Technology to carry out the provisions of this section.".

SEC. 304. INFORMATION SECURITY AND PRIVACY ADVISORY BOARD.

Section 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4), is amended—

(1) in subsection (a), by striking "Computer System Security and Privacy Advisory Board" and inserting "Information Security and Privacy Advisory Board";

(2) in subsection (a)(1), by striking "computer or telecommunications" and inserting "information technology";

(3) in subsection (a)(2)—

(A) by striking "computer or telecommunications technology" and inserting "information technology"; and

(B) by striking "computer or telecommunications equipment" and inserting "information technology";

(4) in subsection (a)(3)—

(A) by striking "computer systems" and inserting "information system"; and

(B) by striking "computer systems security" and inserting "information security";

(5) in subsection (b)(1) by striking "computer systems security" and inserting "information security";

(6) in subsection (b) by striking paragraph (2) and inserting the following:

"(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 through review of proposed standards and guidelines developed under section 20; and";

(7) in subsection (b)(3) by inserting "annually" after "report";

(8) by inserting after subsection (e) the following new subsection:

"(f) The Board shall hold meetings at such locations and at such time and place as determined by a majority of the Board.";

(9) by redesignating subsections (f) and (g) as subsections (g) and (h), respectively; and

(10) by striking subsection (h), as redesignated by paragraph (9), and inserting the following:

"(h) As used in this section, the terms 'information system' and 'information technology' have the meanings given in section 20.".

SEC. 305. TECHNICAL AND CONFORMING AMENDMENTS.

(a) COMPUTER SECURITY ACT.—Subsections (b) and (c) of section 11332 of title 40, United States Code, are repealed.

(b) FLOYD D. SPENCE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2001.—The Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (Public Law 106–398) is amended by striking section 1062 (44 U.S.C. 3531 note).

(c) PAPERWORK REDUCTION ACT.—(1) Section 3504(g) of title 44, United States Code, is amended—

(A) by adding "and" at the end of paragraph (1);

(B) in paragraph (2)—

(i) by striking "sections 11331 and 11332(b) and (c) of title 40" and inserting "section 11331 of title 40 and subchapter II of this chapter"; and

(ii) by striking "; and" and inserting a period; and

(C) by striking paragraph (3).

(2) Section 3505 of such title is amended by adding at the end—

"(c)(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.".

(3) Section 3506(g) of such title is amended—

(A) by adding "and" at the end of paragraph (1);

(B) in paragraph (2)—

(i) by striking "section 11332 of title 40" and inserting "subchapter II of this chapter"; and

(ii) by striking "; and" and inserting a period; and

(C) by striking paragraph (3).

SEC. 306. CONSTRUCTION.

Nothing in this title, or the amendments made by this title, affects the authority of the National Institute of Standards and Technology or the Department of Commerce relating to the development and promulgation of standards or guidelines under paragraphs (1) and (2) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)).

TITLE IV—AUTHORIZATION OF APPROPRIATIONS AND EFFECTIVE DATES

SEC. 401. AUTHORIZATION OF APPROPRIATIONS.

Except for those purposes for which an authorization of appropriations is specifically provided in title I or II, including the amendments made by such titles, there are authorized to be appropriated such sums as are necessary to carry out titles I and II for each of fiscal years 2003 through 2007.

SEC. 402. EFFECTIVE DATES.

(a) TITLES I AND II.—

(1) IN GENERAL.—Except as provided under paragraph (2), titles I and II and the amendments made by such titles shall take effect 120 days after the date of enactment of this Act.

(2) IMMEDIATE ENACTMENT.—Sections 207, 214, and 215 shall take effect on the date of enactment of this Act.

(b) TITLES III AND IV.—Title III and this title shall take effect on the date of enactment of this Act.

TITLE V—CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY

SEC. 501. SHORT TITLE.

This title may be cited as the "Confidential Information Protection and Statistical Efficiency Act of 2002".

SEC. 502. DEFINITIONS.

As used in this title:

(1) The term "agency" means any entity that falls within the definition of the term "executive agency" as defined in section 102 of title 31, United States Code, or "agency", as defined in section 3502 of title 44, United States Code.

(2) The term "agent"—

(A) means an employee of a private organization or a researcher affiliated with an institution of higher learning (including a person granted special sworn status by the Bureau of the Census under section 23(c) of title 13, United States Code) with whom a contract or other agreement is executed, on a temporary basis, by an executive agency to perform exclusively statistical activities under the control and supervision of an officer or employee of that agency; or

(B) means an individual who is working under the authority of a government entity with which a contract or other agreement is executed by an executive agency to perform exclusively statistical activities under the control of an officer or employee of that agency; or

(C) means an individual who is a self-employed researcher, a consultant, or a contractor, or who is an employee of a contractor and with whom a contract or other agreement is executed by an executive agency to perform a statistical activity under the control of an officer or employee of that agency; or

(D) means an individual who is a contractor or who is an employee of a contractor engaged by the agency to design or maintain the systems for handling or storage of data received under this title; and

(E) who agrees in writing to comply with all provisions of law that affect information acquired by that agency.

(3) The term "business data" means operating and financial data and information about businesses, tax-exempt organizations, and government entities.

(4) The term "identifiable form" means any representation of information that permits the identity of the respondent to whom the information applies to be reasonably inferred by either direct or indirect means.

(5) The term "nonstatistical purpose"—

(A) means the use of data in identifiable form for any purpose that is not a statistical purpose, including any administrative, regulatory, law enforcement, adjudicatory, or other purpose that affects the rights, privileges, or benefits of a particular identifiable respondent; and

(B) includes the disclosure under section 552 of title 5, United States Code (popularly known as the Freedom of Information Act) of data that are acquired for exclusively statistical purposes under a pledge of confidentiality.

(6) The term "respondent" means a person who, or organization that, is requested or required to supply information to an agency, is the subject of information requested or required to be supplied to an agency, or provides that information to an agency.

(7) The term "statistical activities"—

(A) means the collection, compilation, processing, or analysis of data for the purpose of describing or making estimates concerning the whole, or relevant groups or components within, the economy, society, or the natural environment; and

(B) includes the development of methods or resources that support those activities, such as measurement methods, models, statistical classifications, or sampling frames.

(8) The term "statistical agency or unit" means an agency or organizational unit of the executive branch whose activities are predominantly the collection, compilation, processing, or analysis of information for statistical purposes.

(9) The term "statistical purpose"—

(A) means the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups; and

(B) includes the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support the purposes described in subparagraph (A).

SEC. 503. COORDINATION AND OVERSIGHT OF POLICIES.

(a) IN GENERAL.—The Director of the Office of Management and Budget shall coordinate and oversee the confidentiality and disclosure policies established by this title. The Director may promulgate rules or provide other guidance to ensure consistent interpretation of this title by the affected agencies.

(b) AGENCY RULES.—Subject to subsection (c), agencies may promulgate rules to implement this title. Rules governing disclosures of information that are authorized by this title shall be promulgated by the agency that originally collected the information.

(c) REVIEW AND APPROVAL OF RULES.—The Director shall review any rules proposed by an agency pursuant to this title for consistency with the provisions of this title and chapter 35 of title 44, United States Code, and such rules shall be subject to the approval of the Director.

(d) REPORTS.—

(1) The head of each agency shall provide to the Director of the Office of Management and Budget such reports and other information as the Director requests.

(2) Each Designated Statistical Agency referred to in section 522 shall report annually to the Director of the Office of Management and Budget, the Committee on Government Reform of the House of Representatives, and the Committee on Governmental Affairs of the Senate on the actions it has taken to implement sections 523 and 524. The report shall include copies of each written agreement entered into pursuant to section 524(a) for the applicable year.

(3) The Director of the Office of Management and Budget shall include a summary of reports submitted to the Director under paragraph (2) and actions taken by the Director to advance the purposes of this title in the annual report to the Congress on statistical programs prepared under section 3504(e)(2) of title 44, United States Code.

SEC. 504. EFFECT ON OTHER LAWS.

(a) SECTION 3510 OF TITLE 44, UNITED STATES CODE.—This title, including amendments made by this title, does not diminish the authority under section 3510 of title 44, United States Code, of the Director of the Office of Management and Budget to direct, and of an agency to make, disclosures that are not inconsistent with any applicable law.

(b) SECTIONS 8, 16, 301, AND 401 OF TITLE 13 AND SECTION 2108 OF TITLE 44, UNITED STATES CODE.—This title, including amendments made by this title, does not diminish the authority of the Bureau of the Census to provide information in accordance with sections 8, 16, 301, and 401 of title 13 and section 2108 of title 44, United States Code.

(c) SECTION 9 OF TITLE 13, UNITED STATES CODE.—This title, including amendments made by this title, shall not be construed as authorizing the disclosure for nonstatistical purposes of demographic data or information collected by the Census Bureau pursuant to section 9 of title 13, United States Code.

(d) SECTION 12 OF THE FEDERAL ENERGY ADMINISTRATION ACT OF 1974.—In accordance with the provisions of this title, data acquired for exclusively statistical purposes under a pledge of confidentiality are exempt from mandatory disclosure in identifiable form for nonstatistical purposes under section 12 of the Federal Energy Administration Act of 1974 (15 U.S.C. 771).

(e) PREEMPTION OF STATE LAW.—Nothing in this title shall preempt applicable State law regarding the confidentiality of data collected by the States.

(f) STATUTES REGARDING FALSE STATEMENTS.—Notwithstanding section 512, information collected by an agency for exclusively statistical purposes under a pledge of confidentiality may be provided by the collecting agency to a law enforcement agency for the prosecution of submissions to the collecting agency of false statistical information under statutes that authorize criminal penalties (such as section 221 of title 13, United States Code) or civil penalties for the provision of false statistical information, unless such disclosure or use would otherwise be prohibited under Federal law.

(g) CONSTRUCTION.—Nothing in this title shall be construed as restricting or diminishing any confidentiality protections or penalties for unauthorized disclosure that otherwise apply to data or information collected for statistical purposes or nonstatistical purposes, including, but not limited to, section 6103 of the Internal Revenue Code of 1986 (26 U.S.C. 6103).

Subtitle A—Confidential Information Protection

SEC. 511. FINDINGS AND PURPOSES.

(a) FINDINGS.—Congress finds the following:

(1) Individuals, businesses, and other organizations have varying degrees of legal protection when providing information to the Federal Government for strictly statistical purposes.

(2) Pledges of confidentiality by the Federal Government provide assurances to the public that information about individuals or organizations or provided by individuals or organizations for exclusively statistical purposes will be held in confidence and will not be used against such individuals or organizations in any Federal Government action.

(3) Protecting the confidentiality interests of individuals or organizations who provide information for Federal statistical programs serves both the interests of the public and the needs of society.

(4) Declining trust of the public in the protection of information provided to the Federal Government adversely affects both the accuracy and completeness of statistical analyses.

(5) Ensuring that information provided for statistical purposes receives protection is essential in continuing public cooperation in statistical programs.

(b) PURPOSES.—The purposes of this subtitle are the following:

(1) To ensure that information supplied by individuals or organizations to an agency for statistical purposes under a pledge of confidentiality is used exclusively for statistical purposes.

(2) To ensure that individuals or organizations who supply information to the Federal Government for statistical purposes will neither have that information disclosed in identifiable form to anyone not authorized by this title nor have that information used for any purpose other than a statistical purpose.

(3) To safeguard the confidentiality of individually identifiable information acquired under a pledge of confidentiality for statistical purposes by controlling access to, and uses made of, such information.

SEC. 512. LIMITATIONS ON USE AND DISCLOSURE OF DATA AND INFORMATION.

(a) USE OF STATISTICAL DATA OR INFORMATION.—Data or information acquired by an agency under a pledge of confidentiality and for exclusively statistical purposes shall be used by officers, employees, or agents of the agency exclusively for statistical purposes.

(b) DISCLOSURE OF STATISTICAL DATA OR INFORMATION.—

(1) Data or information acquired by an agency under a pledge of confidentiality for exclusively statistical purposes shall not be disclosed by an agency in identifiable form, for any use other than an exclusively statistical purpose, except with the informed consent of the respondent.

(2) A disclosure pursuant to paragraph (1) is authorized only when the head of the agency approves such disclosure and the disclosure is not prohibited by any other law.

(3) This section does not restrict or diminish any confidentiality protections in law that otherwise apply to data or information acquired by an agency under a pledge of confidentiality for exclusively statistical purposes.

(c) RULE FOR USE OF DATA OR INFORMATION FOR NONSTATISTICAL PURPOSES.—A statistical agency or unit shall clearly distinguish any data or information it collects for nonstatistical purposes (as authorized by law) by a rule that provides that the respondent supplying the data or information is fully informed, before the data or information is collected, that the data or information could be used for nonstatistical purposes.

(d) DESIGNATION OF AGENTS.—A statistical agency or unit may designate agents, by contract or by entering into a special agreement containing the provisions required by section 502, who may perform exclusively statistical activities, subject to the limitations and penalties described in this title.

SEC. 513. FINES AND PENALTIES.

Whoever, being an officer, employee, or agent of an agency acquiring information for exclusively statistical purposes, having taken and subscribed the oath of office, or having sworn to observe the limitations imposed by section 512, comes into possession of such information by reason of his or her being an officer, employee, or agent and, knowing that the disclosure of the specific information is prohibited under the provisions of this title, willfully discloses the information in any manner to a person or agency not entitled to receive it, shall be guilty of a class E felony and imprisoned for not more than 5 years, or fined not more than $250,000, or both.

Subtitle B—Statistical Efficiency

SEC. 521. FINDINGS AND PURPOSES.

(a) FINDINGS.—Congress finds the following:

(1) Federal statistics are an important source of information for public and private decision-makers such as policymakers, consumers, businesses, investors, and workers.

(2) Federal statistical agencies should continuously seek to improve their efficiency. Statutory constraints limit the ability of these agencies to share data and thus to achieve higher efficiency for Federal statistical programs.

(3) The quality of Federal statistics depends on the willingness of businesses to respond to statistical surveys. Reducing reporting burdens will increase response rates, and therefore lead to more accurate characterizations of the economy.

(4) Enhanced sharing of business data among the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics for exclusively statistical purposes will improve their ability to track more accurately the large and rapidly changing nature of United States business. In particular, the statistical agencies will be able to better ensure that businesses are consistently classified in appropriate industries, resolve data anomalies, produce statistical samples that are consistently adjusted for the entry and exit of new businesses in a timely manner, and correct faulty reporting errors quickly and efficiently.

(5) Congress enacted the International Investment and Trade in Services Act of 1990 that allowed the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics to share data on foreign-owned companies. The Act not only expanded detailed industry coverage from 135 industries to over 800 industries with no increase in the data collected from respondents but also demonstrated how data sharing can result in the creation of valuable data products.

(6) With subtitle A of this title, the sharing of business data among the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics continues to ensure the highest level of confidentiality for respondents to statistical surveys.

(b) PURPOSES.—The purposes of this subtitle are the following:

(1) To authorize the sharing of business data among the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics for exclusively statistical purposes.

(2) To reduce the paperwork burdens imposed on businesses that provide requested information to the Federal Government.

(3) To improve the comparability and accuracy of Federal economic statistics by allowing the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics to update sample frames, develop consistent classifications of establishments and companies into industries, improve coverage, and reconcile significant differences in data produced by the three agencies.

(4) To increase understanding of the United States economy, especially for key industry and regional statistics, to develop more accurate measures of the impact of technology on productivity growth, and to enhance the reliability of the Nation's most important economic indicators, such as the National Income and Product Accounts.

SEC. 522. DESIGNATION OF STATISTICAL AGENCIES.

For purposes of this subtitle, the term "Designated Statistical Agency" means each of the following:

(1) The Bureau of the Census of the Department of Commerce.

(2) The Bureau of Economic Analysis of the Department of Commerce.

(3) The Bureau of Labor Statistics of the Department of Labor.

SEC. 523. RESPONSIBILITIES OF DESIGNATED STATISTICAL AGENCIES.

The head of each of the Designated Statistical Agencies shall—

(1) identify opportunities to eliminate duplication and otherwise reduce reporting burden and cost imposed on the public in providing information for statistical purposes;

(2) enter into joint statistical projects to improve the quality and reduce the cost of statistical programs; and

(3) protect the confidentiality of individually identifiable information acquired for statistical purposes by adhering to safeguard principles, including—

(A) emphasizing to their officers, employees, and agents the importance of protecting the confidentiality of information in cases where the identity of individual respondents can reasonably be inferred by either direct or indirect means;

(B) training their officers, employees, and agents in their legal obligations to protect the confidentiality of individually identifiable information and in the procedures that must be followed to provide access to such information;

(C) implementing appropriate measures to assure the physical and electronic security of confidential data;

(D) establishing a system of records that identifies individuals accessing confidential data and the project for which the data were required; and

(E) being prepared to document their compliance with safeguard principles to other agencies authorized by law to monitor such compliance.

SEC. 524. SHARING OF BUSINESS DATA AMONG DESIGNATED STATISTICAL AGENCIES.

(a) IN GENERAL.—A Designated Statistical Agency may provide business data in an identifiable form to another Designated Statistical Agency under the terms of a written agreement among the agencies sharing the business data that specifies—

(1) the business data to be shared;

(2) the statistical purposes for which the business data are to be used;

(3) the officers, employees, and agents authorized to examine the business data to be shared; and

(4) appropriate security procedures to safeguard the confidentiality of the business data.

(b) RESPONSIBILITIES OF AGENCIES UNDER OTHER LAWS.—The provision of business data by an agency to a Designated Statistical Agency under this subtitle shall in no way alter the responsibility of the agency providing the data under other statutes (including section 552 of title 5, United States Code (popularly known as the "Freedom of Information Act"), and section 552b of title 5, United States Code (popularly known as the "Privacy Act of 1974")) with respect to the provision or withholding of such information by the agency providing the data.

(c) RESPONSIBILITIES OF OFFICERS, EMPLOYEES, AND AGENTS.—Examination of business data in identifiable form shall be limited to the officers, employees, and agents authorized to examine the individual reports in accordance with written agreements pursuant to this section. Officers, employees, and agents of a Designated Statistical Agency who receive data pursuant to this subtitle shall be subject to all provisions of law, including penalties, that relate—

(1) to the unlawful provision of the business data that would apply to the officers, employees, and agents of the agency that originally obtained the information; and

(2) to the unlawful disclosure of the business data that would apply to officers, employees, and agents of the agency that originally obtained the information.

(d) NOTICE.—Whenever a written agreement concerns data that respondents were required by law to report and the respondents were not informed that the data could be shared among the Designated Statistical Agencies, for exclusively statistical purposes, the terms of such agreement shall be described in a public notice issued by the agency that intends to provide the data. Such notice shall allow a minimum of 60 days for public comment.

SEC. 525. LIMITATIONS ON USE OF BUSINESS DATA PROVIDED BY DESIGNATED STATISTICAL AGENCIES.

(a) IN GENERAL.—Business data provided by a Designated Statistical Agency pursuant to this subtitle shall be used exclusively for statistical purposes.

(b) PUBLICATION OF DATA.—Publication of business data acquired by a Designated Statistical Agency shall occur in a manner whereby the data furnished by any particular respondent are not in identifiable form.

SEC. 526. CONFORMING AMENDMENTS.

(a) DEPARTMENT OF COMMERCE.—Section 1 of the Act of January 27, 1938 (15 U.S.C. 176a) is amended by striking "The" and inserting "Except as provided in the Confidential Information Protection and Statistical Efficiency Act of 2002, the".

(b) TITLE 13.—Chapter 10 of title 13, United States Code, is amended—

(1) by adding after section 401 the following:

"§ 402. Providing business data to Designated Statistical Agencies

"The Bureau of the Census may provide business data to the Bureau of Economic Analysis and the Bureau of Labor Statistics ('Designated Statistical Agencies') if such information is required for an authorized statistical purpose and the provision is the subject of a written agreement with that Designated Statistical Agency, or their successors, as defined in the Confidential Information Protection and Statistical Efficiency Act of 2002."; and

(2) in the table of sections for the chapter by adding after the item relating to section 401 the following:

"402. Providing business data to Designated Statistical Agencies.".

I. PURPOSE

H.R. 2458, the bipartisan, "Electronic Government Act of 2002," introduced by Congressman Jim Turner (TX), provides a new framework for managing the Federal government's information resources and increasing the availability of information to citizens through electronic government initiatives. The act establishes an E-Government fund and creates a new Office of Electronic Government in the Office of Management and Budget, which will be led by a presidentially appointed E-Government Administrator. The new office can then focus on better management of our information resources. H.R. 2458 includes several provisions intended to ensure greater citizen access to the Federal government through the improved application of information technology (IT). The act strengthens information security government-wide and addresses the management and protection of information collected for statistical purposes. It also encourages contractor innovation for information technology solutions that will enhance electronic government services and processes, and allows for the limited use of share-in-savings contracts for the procurement of information technology solutions.

II. BACKGROUND AND NEED FOR LEGISLATION

The Federal government, as well as State and local governments, are increasingly turning to the Internet and other information technologies to conduct the business of government. In addition to internal agency electronic initiatives, Federal agencies are conducting paperless acquisitions for goods and services, developing interactive electronic services for the public, and engaging in electronic collection and dissemination of information. Electronic government is the term that captures this use of technology, particularly Web-based Internet applications, to enhance the access to and delivery of government information and services to citizens, businesses, employees, agencies, and other governments.

As the General Accounting Office (GAO) has pointed out: "While the Internet opens new opportunities for streamlining processes and enhancing delivery of services, federal executives and managers must also be cognizant of the responsibilities and challenges that accompany these opportunities. These challenges include (1) sustaining committed executive leadership, (2) building effective e-government business cases, (3) maintaining a citizen focus, (4) protecting personal privacy, (5) implementing appropriate security controls, (6) maintaining electronic records, (7) maintaining a robust technical infrastructure, (8) addressing human capital concerns, and (9) ensuring uniform service to the public." [1] These challenges must be met in order for E-Government initiatives to succeed. Therefore, this act provides for critically needed training for information technology managers, improvements in information security, and facilitates the procurement of information technology solutions.

Congressman Tom Davis noted at the October 1, 2002, Subcommittee on Technology and Procurement Policy mark-up that

[1] "Electronic Government: Challenges Must Be Addressed With Effective Leadership and Management," GAO–01–959T, July 11, 2001.

H.R. 2458 is "strong piece of legislation that will bring an analog federal government into the digital age." It is an amalgam of provisions from several important pieces of legislation that the Committee on Government Reform has developed. Most of these provisions were passed and reported by the Committee, which incorporated them into H.R. 2458 to form a comprehensive approach to the implementation of E-Government initiatives. Among the critical provisions incorporated into this act is S. 803, the Senate companion bill introduced by Senator Joseph Lieberman and passed by the Senate on June 27, 2002, by unanimous consent. This includes several programs to improve the deployment of E-Government, such as the creation of a government-wide Web site, government-wide information collection and dissemination provisions, privacy provisions, and studies on disaster management, the community technology centers, and the digital divide.

The Committee intends this Act to promote streamlining of technology requirements in a way that allows the Federal government to respond to changes in technology in a timely manner, rather than to introduce unnecessary layers of bureaucratic process to the mission of expanding and furthering electronic government. The Committee intends the Act to assist the Federal government in leveraging technology in a way that enhances agency business processes to serve the needs of the citizen.

TITLE I: OFFICE OF MANAGEMENT AND BUDGET ELECTRONIC GOVERNMENT SERVICES

Summary.—In Title I, the act provides several measures to strengthen government-wide approaches to improving the use of information technology for service delivery and governmental efficiency and effectiveness. It establishes an Office of Electronic Government in the Office of Management and Budget (OMB) to focus OMB and government-wide management attention on the important tasks of developing information technology capabilities to enable electronic government initiatives. Second, it endeavors to institutionalize reforms in agency information resources management by establishing a statutory basis for the interagency Chief Information Officers Council. Third, it establishes a program to promote contractor innovation and excellence in E-Gov services and processes. Finally, the act establishes an interagency E-Gov Fund to provide funding for innovative E-Gov initiatives.

The major impetus for the provisions of Title I is the repeated call for improved leadership for electronic government. Currently, Federal information resources management (IRM) is overseen by OMB's Office of Information and Regulatory Affairs (OIRA) under the Paperwork Reduction Act, 44 U.S.C. ch. 35. Over the years, there have been many complaints about agency IRM practices and OIRA IRM oversight.[2]

Rather than address the challenges of electronic government through review and perhaps revision of the IRM framework in the

[2] See, for example, "Paperwork Reduction Act Reauthorization and Government Information Management Issues," Congressional Research Service, RL30590, February 7, 2001, and "Information Resources Management: Comprehensive Strategic Plan Needed to Address Mounting Challenges," General Accounting Office, GAO–02–292, February 2002; "Paperwork Reduction Act of 1995," Report of the Committee on Government Reform and Oversight, House of Representatives, Report 104–37, February 15, 1995.

Paperwork Reduction Act, the current legislation reflects a decision to establish a separate office and management approach for E-Gov. Given the pressing nature of the problems the legislation addresses, and given the broad support for this approach in both this body and the Senate, the Committee supports the effort at this time, with reservation. The Committee will watch the implementation of these provisions very closely, however, to assess whether they actually improve Federal management of information resources.

Definitions.—This Title uses the definitions provided in 44 U.S.C. 3502, but provides eight additional definitions, including "electronic government" and "enterprise architecture." The Committee intends the definition of "electronic government" to be interpreted as applying to agency information technologies in the same manner as is applied to information technology under the Clinger Cohen Act, including appropriate exemptions in that statute for national security systems.

The Committee defines the term "enterprise architecture" because successful public and private-sector organizations have used such architectures as best practice for effective business and technology transformation. In simplest terms, an enterprise represents the entire scope of an entity (e.g., an entire agency or set of agencies performing a related function), and an architecture is the structural description of the processes that make up the entity; an "enterprise architecture" describes the business, information, technology, and infrastructure of such entities. The architecture describes the current, or "as is," environment, as well as the target, or "to be," environment, and the modernization plan that bridges the two. When well implemented, enterprise architectures bring clarity to the interrelationships among business operations and the underlying IT that support the operations, and can be used to guide IT investments in a way that reduces redundancies in systems and processes, modernizes operations, and improves program performance.

Categorization Standards and Guidelines.—The E-Government Administrator will assist the OMB Director in establishing policies to support IT standards and guidelines. The Committee intends that the standards and guidelines to be developed by the National Institute of Standards and Technology for the categorization of Federal Government electronic information shall be consistent with the recommendation for any similar standards required in Section 207(d) of this Act.

Ongoing Dialogue.—The Office of Electronic Government sponsor ongoing dialogue that shall be conducted among Federal (in the executive, legislative, and judicial branches), State, local, and tribal government leaders on electronic Government to encourage collaboration and enhance understanding of best practices and innovative approaches in acquiring, using, and managing information resources.

Chief Information Officers Council.—The Committee recognizes that as technology and management priorities change, the agenda of the CIO Council must allow for flexibility. The functions of the Council that this bill describes are intended to be sufficiently broad so as to provide OMB and CIOs with flexibility to address and manage change so that the Administration can adjust the priorities of the Council accordingly.

E-Government Fund.—The act establishes an interagency E-Gov Fund to provide funding for innovative E-Gov initiatives. Section 3604 outlines criteria by which projects submitted to for funding from this Fund are to be evaluated. The Committee notes that OMB must "consider" certain criteria under 3604(c)(1), but that applying each of these criteria is not mandatory in every case and projects should be evaluated by relevant criteria. The Committee also notes that these criteria will evolve to meet the needs of electronic government, and that the Office of Electronic Government shall be responsible for ensuring that the criteria for evaluating projects applying for funds reflect changes to the government's electronic government initiatives.

TITLE II: FEDERAL MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

Summary

Title II mandates a broad array of specific initiatives that require the use of Internet applications and other information technologies to enhance Federal E-Government capabilities. Among its provisions are requirements to support broader use of electronic signatures, develop a Federal Internet portal, improve public access to public information in Federal agencies and the courts, strengthen privacy protections, improve Federal workforce information technology skills, to harness the innovative spirit of the private sector by making greater use of share-in-savings contracts, research the use of information technologies for better crisis management, and mandate more effective use of community technology centers.

The spectacular growth of the Internet and the increasing use of information technology applications by government agencies not only have fueled a drive for broad government-wide reforms to promote E-Gov, but also have provided insights into opportunities for specific E-Gov initiatives. The following provisions are necessary to ensure the implementation of the concepts outlined and promoted in this act.

Agency Responsibilities

Title II establishes agency responsibilities for implementing this act, including the development of performance measures to help agencies ensure that the E-Government initiatives will enable progress toward agency objectives. Agencies are required to report to OMB on their compliance with the act's provisions. The agencies are instructed to consider the impact of E-Government initiatives on citizens without access to the Internet and to ensure that the availability of government information resources is not diminished for such persons.

Accessibility to People with Disabilities.—The Committee intends that the term "information technology" in this Section be interpreted in the same manner as the term "Electronic and Information Technology" under Section 508 of the Rehabilitation Act of 1973, as amended.

E-government Status Report.—The Committee notes that in preparing for this annual reporting requirement, that agencies should report on the sections of this Act that are relevant to agency activities and initiatives, unless noted. Further, as many electronic gov-

ernment initiatives involve cross-agency collaboration, the Committee intends that cross-agency initiatives be included in the report. In cases where agencies are involved in collaborative efforts, one agency may serve as the lead agency in reporting on the status of the imitative on behalf of its partner agencies.

Public Access

Provisions in this section are intended to increase the availability of information and the ease with which the public may access it. Sifting through the wealth of information disseminated by the government can be daunting and confusing. Currently, the federal government organizes publicly available information according to agency jurisdiction which often leads to duplicative information resource management efforts, and may be counter-intuitive for citizens conducting searches.

This Act requires federal agencies to improve online access to agency information through a number of initiatives. For instance, the federal Internet portal will help improve public access to government information and services. The Committee intends that access to information on a portal web site be consistent with existing laws and policies on privacy. Portal web sites maintained by Federal agencies should only allow access to information on individuals if such access fully complies with privacy protections under existing law and policy. A directory of government websites organized by subject matter, will be created and linked to the federal Internet portal. Furthermore, regulatory agencies will be required to include on a publicly accessible website all information required to be published in the Federal Register and to keep public rulemaking information online. Federal Courts will be required to have information and judicial opinions on websites.

OMB will be responsible for providing guidance to agencies in a number of areas so that they may improve the organization, presentation, and public accessibility of their information, including information on the Internet. OMB must establish an Interagency Committee on Government Information which will submit its recommendations to OMB about information access, dissemination, and retention. OMB must then issue policies to address such matters as standards for the organization and categorization of government information in a way that is searchable electronically and interoperable across agencies. OMB must also issue guidance to agencies regarding the content requirements and accessibility of their websites.

Electronic Docketing.—Subsection (d) requires agencies, "to the extent practicable," to include submissions under section 553(c) of title 5, U.S.C., and other materials that agencies include in their dockets (by rule or practice) in their electronic dockets, "whether or not submitted electronically." The Committee intends that this requirement serve to increase transparency for agency rulemaking by making agency dockets accessible online wherever possible. The Committee notes that agencies receive many materials in the docket that may be difficult to make accessible through electronic means. There are also copyright issues associated with some materials submitted to agency dockets. To avoid the burden associated with transferring certain items to electronic format, such as books or physical objects, agencies may simply provide notice of the avail-

ability of the material, including in the electronic docket a description of the item and instructions for the public on accessing the material through the agency docket. Agencies may also consider using visual means, such as digital photos, to make materials available through the agency's electronic docket.

Section 207 "Accessibility, Usability, and Preservation of Government Information"

Process.—The Committee notes that the activities of the Interagency Committee outlined in this section will lead to further actions, and uses this opportunity to clarify this process. In all cases, the Interagency Committee is charged with making recommendations to OMB and/or the Executive Branch agency with authorities in that topic area. OMB will then develop and issue guidance and/or policy based on the recommendation of the Committee. Federal agencies are then responsible for implementing those guidelines/policies. Information placed on government web sites can be federal records; federal records should be routinely reviewed to assure proper scheduling for archival storage.

Consultation of the Interagency Committee.—The Committee intends that the consultation of the Interagency Committee on Government Information with interested groups be done in such a way as to simply seek views and not to warrant the establishment of a Federal Advisory Committee. The Committee does not contemplate the consultation activities of the Interagency Committee to provide advice that would invoke the Federal Advisory Committee Act (FACA)

Searchable Identifiers.—The Committee intends that the searchable identifiers developed under this section will build on an advance the purposes of Section 3511 of title 44 of the United States Code.

Privacy

The revolutionary impact of the Internet and the growing number of online transactions raise concerns about the protection of information collected in an "identifiable form," that is information that permits the identity of the individual to whom the information applies to be reasonably inferred directly or indirectly.

Privacy Impact Assessments.—This section requires agencies, with OMB guidance, to complete Privacy Impact Assessments (PIA) before collecting information in an identifiable form or procuring information technology that collects, maintains, or disseminates such information. The Committee intends that the OMB guidance on for conducting Privacy Impact Assessments (PIAs) under Section 208(b) address initial, high-level assessments that are consistent with post-procurement PIAs done by some agencies.

In addition, the Committee intends that the OMB guidance on process for developing a Privacy Impact Assessment (PIA) be done in a way that allows for consistency with work done by agencies to assess privacy requirements under the Paperwork Reduction Act (PRA) and the Privacy Act of 1974, with regard to new collections of information that include personally identifiable information.

In section 208(b)(1)(B)(iii), the Committee intends that on occasions where a Privacy Act systems of record notice is required, agencies can satisfy the publication requirement for PIAs by at-

taching a PIA to a Privacy Act systems of records notice published in the Federal Register.

OMB must also issue guidance regarding the posting of privacy notices on agency websites. This will give the public a better understanding of what and why information is collected, its use, with whom it will be shared, individual rights with regard to the information, and how it will be secured. Additionally, OMB guidance will cover the conversion of privacy policies into machine-readable formats to provide the public with a simple automated way to better control the use of personal information on websites they visit.

Tracking.—In addition, the Committee intends this Act to be consistent with OMB policy and the restrictions on the tracking of individuals through agency websites through the use of such devices as persistent cookies.

Information technology training

E-Government initiatives require a well-trained information technology workforce to implement them. However, in 2001 the General Accounting Office added the Federal government's human capital management crisis to its annual high-risk list. The expected personnel shortages are greatest in the information technology fields. In fact, fifty percent of the federal government's information technology workforce will be eligible to retire by 2006, compared to 34 percent government-wide. Therefore, it is critical that the federal government retains and recruits talented IT workers, but the competition from the private sector is fierce. Currently, federal agencies face overwhelming obstacles in enticing IT workers away from the private sector and into the federal workforce. The federal government simply cannot compete with the salaries, benefits, and comprehensive training offered by the private sector. For these reasons, the act creates training opportunities in information technology management through the Digital Tech Corps, an exchange of eligible mid-level staff between leading-edge private sector organizations and governmental agencies. The Digital Tech Corps program is intended to invigorate the current IT workforce and help establish the Federal government as a desirable employer in the IT arena. This program is based on H.R. 3925, the Digital Tech Corps Act of 2002, which the Committee on Government Reform favorably reported by voice vote on March 14, 2002.

Technical innovations

In order to evaluate the overwhelming number of industry proposals offering solutions to the Federal government's IT challenges, this act includes technical innovation provisions based on H.R. 4629, introduced by Congressman Tom Davis on May 1, 2002. The E-Government Administrator will establish a multi-agency screening board to review and assess cutting-edge technologies that promise to facilitate and enhance the rapid deployment of IT solutions that will breakdown stovepipes and achieve greater interagency cooperation. The screening board will then submit its assessments to the E-Government Administrator for funding consideration under the E-Government Fund or will forward them to the appropriate agency. These provisions are an excellent means to leverage innovative technology solutions that would not otherwise be available to the government.

Share-in-savings

To date, congressional reforms of the government procurement process include streamlining measures, cost-savings, access to technological advancements, and reduced procurement cycles. As a result there has been an improvement in the quality of products and services purchased by the federal government. However, these reforms do not address the growth in agency purchases of services necessary to meet their mission objectives, particularly in the IT field. Therefore, this act will authorize the government-wide use of share-in-savings contracts for information technology.

Share-in savings is an innovative contract vehicle that allows agencies to leverage their limited resources in order to achieve a greater return on investment. Agencies can use this type of contract to improve their service delivery and lower their costs without initial capital expenditures since the contractor would provide the technology. Further, agencies would be obligated to pay the contractor for the services only if savings are realized and then payment is limited to an agreed upon portion of the total savings realized. The agency may retain a portion of the remaining savings. Agencies would be permitted to enter into share-in-savings contracts for five years, and with appropriate approval up to 10 years. The share-in-savings provisions would sunset in September 2009. The federal government may use an aggregate of five such contracts during fiscal years 2003, 2004, and 2005. Beginning in fiscal year 2006, the aggregate number would increase to ten. Two years after enactment, the Office of Management and Budget is required to report to Congress on the number of share-in-savings contracts entered into and its recommendations for changes in law to encourage their use. The General Accounting Office is required to review the OMB report. It is the hope of the Committee that OMB will encourage federal agencies to engage in these contracts and contact the Administrator of General Services for guidance in identifying share-in-savings contract opportunities as directed under these provisions. The share-in-savings concept originated in H.R. 3832, the Services Acquisition Reform Act (SARA). The Subcommittee on Technology and Procurement Policy held a legislative hearing on SARA on March 7, 2002.

Integrated reporting study and pilot projects

The Committee notes that this section is consistent with the Administration's approach to consolidation of information by collection of information one time, and using such information to populate data elements that can be utilized across many purposes and transactions. By "collect once, use many," the Administration seeks to reduce stovepipes and to reduce the reporting burdens on citizen and businesses. The Committee understands that the Administration's electronic government initiatives will demonstrate methods by which this principle can be realized, while ensuring the security and privacy of personal information.

Contents of study on enhancement of crisis response

The Committee intends that the contents of the commissioned study examine opportunities for research and development on enhanced technologies for improving communications with citizens at risk before and during a crisis; enhancing the use of remote sensor

data and other information sources for planning, mitigation, response, and advance warning; building more robust and trustworthy systems for communications in crises; facilitating coordinated actions among responders through more interoperable communications and information systems; and other areas of potential improvement as determined during the course of the study.

Disparities in access to the Internet

In our efforts to modernize the government's information resources management and implement E-Government initiatives, we must bear in mind that not all citizens have Internet access. Therefore, the act requires the General Services Administration to commission a study to examine the disparities in Internet access, including a review of alternative sources of internet access, particularly access through public libraries. The study must include recommendations for ensuring that E-Government initiatives do not decrease public access to government information. The Committee intends that the commissioned study should examine disparities in Internet access, including a review of alternative sources of internet access, particularly access through public libraries.

TITLE III: INFORMATION SECURITY

A. Summary

Title III of H.R. 2458 is the "Federal Information Security Management Act of 2002" (FISMA). It is intended to revise GISRA, the Government Information Security Reform provisions of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (Div. A, Title X, Subtitle G, sec. 1061–1065; Pub. L. 106–398, October 30, 2000).

The purpose of FISMA is to permanently authorize a government-wide risk-based approach to information security by eliminating GISRA's two-year sunset, and to further strengthen Federal information security by requiring compliance with minimum mandatory management controls for securing information and information systems, clarifying and strengthening current management and reporting requirements, and strengthening the role of National Institute of Standards and Technology (NIST).

In accomplishing this range of reforms, FISMA takes the significant step of consolidating current information security requirements spread across the GISRA, the Computer Security Act, the Clinger-Cohen Act, and the Paperwork Reduction Act. FISMA eliminates obsolete mandates, updates outmoded provisions, harmonizes overlapping requirements, and strengthens key requirements. The result is a clearer and stronger law to guide Federal agencies to provide needed improvements to their information security.

Title III largely reflects the provisions of H.R. 3844, introduced on March 5, 2002, by Representative Tom Davis, for himself and Representative Steve Horn. Following introduction, H.R. 3844 was referred to the Committees on Government Reform and the Committee on Science. Several legislative hearings were held:

- On March 6, 2002, the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Rela-

tions held a hearing, Lessons Learned from the Government Information Security Reform Act of 2000.

• On May 2, 2002, the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations and the Subcommittee on Technology and Procurement Policy held a joint hearing on H.R. 3844.

• On July 10, 2002, the Committee on Government Reform voted to accept a revised version of H.R. 3844 as an amendment to H.R. 5005, the Homeland Security Act. On July 26, 2002, a somewhat further modified version of the legislation was accepted as a floor amendment to H.R. 5005. As thus amended, H.R. 5005 was passed by the House of Representatives on July 26, 2002.

• On October 9, 2002, an again slightly modified version of H.R. 3844 was considered by the Committee on Government Reform, as Title III of the instant legislation, H.R. 2458.

B. Background and Need for the Legislation

Increases in computer interconnectivity, especially through the Internet, continue to revolutionize the way our government, our nation, and much of the world communicate and conduct business. Unfortunately, this interconnectivity has also dramatically increased significant risks to our computer systems and the critical operations and infrastructures they support, such as telecommunications, power distribution, public health, national defense and law enforcement.

As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital governmental and national interests. Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, including for reasons of crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and foreign intelligence services are learning to use tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to information and systems. These growing threats are in addition to the continuing problem faced by all organizations from disgruntled insiders who often have the knowledge to gain access and inflict damage or steal assets, even if they do not know a great deal about computers.

Over the past several years, GAO has reported numerous times that poor information security is a widespread federal problem with potentially devastating consequences.[3] Although agencies have taken steps to redesign and strengthen their information system

[3] U.S. General Accounting Office, Information Security: Opportunities for Improved OMB Oversight of Agency Practices. GAO/AIMD–96–110 (Washington, D.C.: Sept. 24, 1996). U.S. General Accounting Office, Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk, GAO/AIMD–98–92 (Washington, D.C.: Sept. 23, 1998); Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies, GAO/AIMD–00–295 (Washington, D.C.: Sept. 6, 2000). U.S. General Accounting Office, Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets, GAO–02–231T (Washington, D.C.: Nov. 9, 2001).

security programs, GAO analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations.[4]

The weaknesses GAO identified place a broad array of federal operations and assets at risk. For example:

- Resources, such as federal payments and collections, could be lost or stolen;
- Computer resources could be used for unauthorized purposes or to launch attacks on others;
- Sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information, could be inappropriately disclosed or browsed or copied for purposes of espionage or other types of crime;
- Critical operations, such as those supporting national defense and emergency services, could be disrupted;
- Data could be modified or destroyed for purposes of fraud or disruption; and
- Agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, on October 30, 2000, the Congress enacted GISRA, the Government Information Security Reform provisions of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (Div. A, Title X, Subtitle G, sec. 1061–1065; Pub. L. 106–398, October 30, 2000). GISRA supplements information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996. GISRA drew on these separate requirements to establish an overall framework for managing information security centered on the establishment of agency-wide information security management programs involving periodic risk assessments and periodic management testing and evaluation; and annual independent evaluation of each agency's information security program and practices.

GAO has reported that the first-year implementation of GISRA yielded significant benefits in terms of agency focus on information security.[5] Agency Inspectors General (IG) also have described GISRA as a positive step toward improving information security particularly by increasing agency management's focus on this issue. However, GAO and IG's have also reported on problems in implementing GISRA, as well as the potential problems created by the expiration of GISRA on November 29, 2002.

---

[4] U.S. General Accounting Office, High-Risk Series: Information Management and Technology, GAO/HR–97–9 (Washington, D.C.: Feb. 1, 1997); High-Risk Series: An Update, GAO/HR–99–1 (Washington, D.C.: Jan. 1999); High Risk Series: An Update, GAO–01–263 (Washington, D.C.: Jan. 2001).

[5] U.S. General Accounting Office, Information Security: Additional Actions Needed to Fully Implement Reform Legislation. GAO–02–470T. (Washington, D.C.: March 6, 2002). U.S. General Accounting Office, Information Security: Comments on the Proposed Federal Information Security Management Act of 2002. GAO–02–677T. (Washington, D.C.: May 2, 2002).

GAO has identified several key issues that remain a problem for federal information security under GISRA. Currently, agencies have wide discretion in deciding what computer security controls to implement and the level of rigor with which to enforce these controls. In theory, some discretion is appropriate since, as OMB and NIST guidance state, the level of protection that agencies provide should be commensurate with the risk to agency operations and assets. In essence, one set of specific controls will not be appropriate for all types of systems and data. Nevertheless, GAO studies of best practices at leading organizations have shown that more specific guidance is important.[6] In particular, specific mandatory standards for specified risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; help ensure that shared data are appropriately and consistently protected; and reduce demands for already limited agency information security resources to independently develop security controls.

The Congress should have consistent and timely information for overseeing agencies' efforts to implement information security requirements and for taking corrective actions, as well as for budget deliberations. Unfortunately, both GAO and the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations have experienced difficulties in getting access to information concerning agency implementation of GISRA. Clarified statutory language, including more precise reporting requirements should help ensure that Congress receives the information it needs to perform its oversight function.

Experience under GISRA has also highlighted a number of other provisions that complicate fulfillment of the law's purposes. There is significant variation among agencies in structuring their agency information security programs, and not all agencies have well-established information security offices. Reliance on different provisions in GISRA have led to some confusion about requirements for information security "programs" as opposed to "plans", as well as "mission critical systems." Agencies also continue to lack adequate plans and procedures to respond to information security incidents and ensure the continuity of operations for information systems that support the operations and assets of the agency.

The imminent expiration of GISRA along with identified Federal information security weaknesses not adequately addressed under current law argues for legislation to strengthen Federal information security.

C. Explanation of the Legislation

Title III, entitled the "Federal Information Security Management Act of 2002" (FISMA), largely reflects the provisions of H.R. 3844, introduced on March 5, 2002, by Rep. Tom Davis, for himself and Rep. Steve Horn. The provisions amend the Government Information Security Reform (GISRA) provisions of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (Div. A, Title X, Subtitle G, sec. 1061–1065; Pub. L. 106–398, October 30, 2000).

[6] GAO/AIMD–98–68, May 1998.

FISMA is composed of GISRA revisions, provisions of the "Federal Information Policy Act of 2000" (H.R. 5024), introduced on July 27, 2000, by Rep. Tom Davis (R–VA), and the original GISRA legislation, the "Government Information Security Act of 1999 (S. 1993), introduced on November 19, 1999, by Senator Fred Thompson (R–TN) and Senator Joseph Lieberman (D–CT). The legislation also includes elements similar to provisions in the "Computer Security Enhancement Act of 2001" (H.R. 1259), introduced on March 28, 2001 (and passed by the House on November 27, 2001), by Rep. Connie Morella (R–MD).

In summary, FISMA:

- Permanently authorizes the government-wide risk-based approach to information security by striking the current 44 U.S.C. 3536, thus eliminating GISRA's two-year sunset;
- Strengthens Federal information security by requiring compliance with minimum mandatory management controls for securing information and information systems to manage risks as determined by agencies;
- Improves accountability and congressional oversight by clarifying agency reporting requirements and ensuring access to information security evaluation results by the GAO;
- Improves compliance by streamlining a number of GISRA requirements and clarifying inconsistent and unclear terms and provisions;
- Clarifies provisions regarding responsibilities for national security systems;
- Improves Federal information security by strengthening the role of NIST; and
- Streamlines statutory requirements by repealing duplicative provisions in the Computer Security Act and the Paperwork Reduction Act.

Overall, the goal of FISMA is to continue and strengthen the risk management information security reforms first enacted into law in GISRA. This goal is accomplished through six key sets of provisions.

First, in § 3533, FISMA sets out OMB's information security responsibilities. In one respect, FISMA expands OMB responsibilities provided under GISRA, requiring OMB to promulgate information security standards developed by NIST. By this change, OMB would take over this function from the Secretary of Commerce, who would still promulgate NIST-developed information system standards. Otherwise, FISMA refines the comparable GISRA section to streamline the OMB provisions and avoid unnecessary duplication with other provisions of law.

Second, in § 3534, FISMA sets out Federal agency information security responsibilities. Again, FISMA maintains the general range of agency responsibilities provided under GISRA, while refining specific provisions to streamline provisions and more clearly specify key requirements, for example, providing more detailed requirements for the agency information security office, and responsibilities for periodic management testing and evaluation.

Third, in § 3535, FISMA provides for annual independent evaluation of agency information security programs and practices. Preserving the general scheme established under GISRA, FISMA refines the requirements of this section to address concerns raised by

agency program and Inspectors General officials about the scale and scope of the annual evaluation. The overall goal of FISMA's revision is to ensure accountability for a comprehensive evaluation of agency information security. This does not require a single simultaneous or integrated review of all systems. Rather, the Committee envisions a set of reviews involving testing of systems with different standards of frequency and rigor depending on risk levels and unique requirements, including those for national security systems. Thus, each agency's annual information security evaluation should be comprehensive in its scope while selective in its detail. The goal is to ensure accountability for a review or set of reviews that in combination covers the full extent of an agency's information security program and practices. Given the Committee's concern that these evaluations be carried out in a way that provides meaningful review and accountability without jeopardizing efficient and effective operations of either agency program operations, agency IG's, or OMB, the Committee expects OMB to report on the costs and benefits of this process.

Fourth, in § 3536, FISMA provides for the operation of a central Federal information security incident center. The Committee recognizes the current successful operation of GSA's incident center, FedCIRC. The purpose of the requirement in this section is to provide a permanent authorization for a center such as FedCIRC, and to insure that its activities are broadly conceived and faithfully carried out consistent with the mandate in this section. Testimony by GAO and others in both the context of government information security and critical infrastructure protection have stressed the importance of having a well-established government-wide incident center that can analyze security incidents, provide timely assistance, and consult with agencies across the entire range of government, including national security agencies, to ensure an effective government-wide response to information security threats and vulnerabilities. The Committee believes the statutory mandate in this section will accomplish this goal.

Fifth, in § 3537, FISMA places national security systems within the government-wide information security risk management framework of the legislation. The purpose of the section is to make clear that while agencies must manage national security systems consistent with applicable national security requirements (independent of OMB or NIST system requirements), they must also secure those systems with the same risk-based management approach and the same commitment to agency accountability applicable to all Federal agencies through provisions of the instant legislation, most notably the requirements at § 3534 and § 3535.

This section is intended to complement other provisions that address the unique needs of national security systems within the framework of a government-wide approach to information security, while at the same time simplify GISRA's varied formulations for national security-related systems. For example:

- FISMA's § 3532 replaces GISRA's "mission critical system" definition with a "national security system" definition that encompasses the two traditional components of national security-related systems: (1) the so-called "Warner Amendment" national security systems, most recently enacted into law in section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 11103);

and (2) the Computer Security Act's description of systems protected by procedures for classified information (15 U.S.C. 278g–3(a)(3)). This revision restores the longstanding statutory treatment of military and intelligence mission-related systems and classified systems.

• FISMA's § 3533 limits OMB authority over national security systems to oversight and reporting to Congress. This parallels FISMA's sec. 303, which continues the Computer Security Act's exemption of national security systems from NIST-developed standards.

• FISMA's § 3535 similarly revise GISRA to eliminate unnecessarily complicated provisions, while maintaining protections for national security systems. It clarifies procedures for evaluating national security systems within the context of agency-wide evaluations and strikes the GISRA requirements for audits of national security system evaluations. FISMA clearly requires agencies, as well as evaluators, to take all appropriate steps necessary to protect the security of national security systems. Furthermore, as under GISRA, FISMA provides that agencies responsible for national security systems have complete discretion in choosing entities to perform the required independent evaluations. The Committee believes that these and the other steps provide ample protection for national security systems and for the agencies responsible for them. An additional audit process neither is necessary to provide protection nor would produce any information of value to assessing the adequacy and effectiveness of any information security program or practice.

Sixth, FISMA would require the development, promulgation, and compliance with minimum mandatory management controls for securing information and information systems to manage risks as determined by agencies. Specifically:

• Under the amendments to the NIST Act in sec. 303, FISMA would maintain NIST's current standards development mission, but would require NIST to develop: (1) standards for categorizing information according to information security control objectives and risk levels; and (2) minimum information security requirements for each information category. FISMA also would strengthen NIST's research and technical assistance role.

• Under the amendments to the Clinger-Cohen Act in section 302, OMB would issue information security standards based on the NIST-developed standards and would require agencies to comply with them. This increases OMB's information security authority, given that the Secretary of Commerce is currently required by the Computer Security Act to issue such standards. The Secretary of Commerce would retain the responsibility for promulgating NIST-developed information system standards.

• Under § 3534, agencies would have to comply with the OMB-promulgated information security standards, and the use of more stringent protections would have to be consistent with the NIST/OMB standards. To achieve greater consistency within and across agencies, waivers of the standards are not permitted. These requirements are intended to provide a con-

sistent information security approach across all agencies, while meeting the mission-specific needs of each agency.

It should be noted that in this section FISMA refers to "security" instead of "security and privacy," as under the Computer Security Act. The elimination of references to privacy reflects the decision to have NIST focus on technical issues critical to developing effective information security controls. While the Computer Security Act linked security and privacy, experience over the last decade and a half has shown that privacy policy is largely outside the area of expertise of NIST. This is a reflection of the differences between information security and privacy. Information security requires the development and use of technical and management controls and processes to provide appropriate levels of information integrity, confidentiality, and availability. Without adequate security, personal information is, of course, vulnerable to a breach of privacy, but the protection of privacy flows from policy decisions about levels of confidentiality to apply to specific sets of personal information. Thus, the congressional Office of Technology Assessment stated in 1995, "Privacy refers to the social balance between an individual's right to keep information confidential and the societal benefit derived from sharing information, and how this balance is codified to give individuals the means to control personal information." Issue Update on Information Security and Privacy in Network Environments, June 1995. The development of such policy choices is not a technical matter for an agency such as NIST. On the other hand, attention to standards and guidelines necessary to provide agreed upon confidentiality in information systems is a matter for the agency.

The Committee believes that the provisions of FISMA can significantly strengthen information security in the Federal government. The Committee's view is that while the initial implementation of GISRA has been beneficial, the changes provided in this title can drive further reforms in Federal information security. This legislation is needed therefore not simply to remove the sunset that will otherwise soon end GISRA, but also to reinforce and redouble the Federal government's commitment to establishing information security as an integral part of its operations.

TITLE IV: AUTHORIZATION OF APPROPRIATIONS AND EFFECTIVE DATES

Title IV provides authorization of appropriations and effective dates for this legislation.

TITLE V: CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY

This act establishes new processes for the improved accuracy, management, and protection of information collected from businesses for statistical purposes. It lifts the current statutory barriers on information sharing of business-related statistical data between the Census Bureau, the Bureau of Labor Statistics, and the Bureau of Economic Analysis so that the Federal government can improve accuracy and correct anomalies in economic statistics. Additionally, the act would reduce the reporting burdens on the businesses that must now supply data separately to the individual agencies. The data-sharing will be conducted according to written agreements that will specify its uses, including which data is to be used and

the appropriate security safeguards that will be followed. The Act will also ensure that the confidential data that individual citizens and businesses provide to Federal agencies for statistical purposes are subject to uniform and rigorous confidentiality protections. The Act includes severe fines and penalties for willful disclosure of collected data. These provisions originated in H.R. 5215, the Confidential Information Protection and Statistical Efficiency Act of 2002, which passed by voice vote in the Committee on Government Reform on October 9, 2002.

III. Legislative Hearings and Committee Action

H.R. 2458, the bipartisan "E-Government Act of 2001" was introduced on July 11, 2001, by Congressman Jim Turner (TX), the Ranking Member of the Government Reform Subcommittee on Technology and Procurement Policy. As introduced, the legislation largely reflected the provisions of Title I and II of the current Act. After introduction, the bill was referred to the Government Reform and the Subcommittee on Technology and Procurement Policy.

On September 18, 2002, the Subcommittee on Technology and Procurement Policy held a legislative hearing to consider the legislation and S. 803, the Senate companion bill, which was passed by the Senate on June 27, 2002. The Subcommittee heard testimony from Linda Koontz of GAO; Mark Forman from the Office of Management and Budget; Pat McGinnis from the Council of Excellence in Government; Mr. Tom Gann, Vice President of Government Relations for Siebel Systems testifying on behalf of the Information Technology and Industry Council, and Mr. Roger Baker, former Chief Information Officer of the Department of Commerce.

On October 1, 2002, the Subcommittee held a mark-up of the bill. Subcommittee Chairman Tom Davis offered three amendments that were accepted by voice vote. The first amendment strikes the Senate confirmation requirement for the Administrator of Electronic Government. The second amendment increases training opportunities for IT managers through the creation of the Digital Tech Corps, which will encourage the exchange of talented mid-level staff between leading-edge private sector organizations and governmental agencies. The third amendment authorizes the government-wide use of share-in-savings contracts for information technology solutions. These amendments were incorporated into a manager's amendment in the nature of a substitute that the Subcommittee approved by voice vote. This substitute reflected the current form of the legislation, namely, Titles I, II, III, IV, and V.

On October 9, 2002, the Committee on Government Reform held a business meeting where it marked up H.R. 2458. The Committee, by voice vote, did not accept an amendment offered by Congressman Jim Turner to reinstate Senate confirmation of the Administrator of Electronic Government. By voice vote, the Committee then approved reporting H.R. 2458 without amendment to the full House.

IV. Section-by-Section Analysis

SECTION 1. SHORT TITLE; TABLE OF CONTENTS

This Act may be cited as the "E-Government Act of 2002."

SEC. 2. FINDINGS AND PURPOSES

(a) Findings

This subsection lists seven findings including: (1) that the use of computers and the internet is transforming the relationships among citizens, private businesses, and the Government, (2) that the Federal Government has had uneven success in applying advances in information technology to enhance it services and functions, (3) that most Internet services of the Federal Government have been developed and presented separately, according to the jurisdictional boundaries of the individual department or agency rather than being integrated cooperatively according to function or topic, and (4) that to take full advantage of improved Government performance that can be achieved through Internet-based technology requires strong leadership, better organization, improved interagency collaboration, and more focused oversight of agency compliance with statutes related to information resources management.

(b) Purposes

This subsection lists 11 purposes of the Act, including: (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 (OMB), (2) to improve the ability of the Government to achieve agency missions and program performance goals, (3) to promote the use of the Internet and emerging technologies within and across the Government agencies to provide citizen-centric Government information and services, (4) to promote access to high quality Government information and services across multiple channels and (5) to transform agency operations by utilizing, where appropriate, best practices from public and private sector organizations.

TITLE I—OFFICE OF MANAGEMENT AND BUDGET ELECTRONIC GOVERNMENT SERVICES

SEC. 101. MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

This section creates a new chapter 36 in title 44, U.S. Code, entitled "Management and Promotion of Electronic Government Services." This chapter follows the Paperwork Reduction Act (PRA), which comprises chapter 35 in title 44. The new chapter 36 has six sections:

- § 3601. Definitions;
- § 3602. Office of Electronic Government;
- § 3603. Chief Information Officers Council;
- § 3604. E-Government Fund;
- § 3605. Program to Encourage Innovative Solutions to Enhance Electronic Government Services and Processes; and
- § 3606. E-Government Report.

This section establishes an OMB Office of Electronic Government, headed by an Administrator of Electronic Government, to provide overall leadership and direction to the executive branch on electronic Government initiatives. The E-Gov Administrator would

be appointed by the President. The E-Gov Administrator will coordinate E-Gov efforts with the Administrator of the Office of Information and Regulatory Affairs (OIRA) to ensure consistent implementation of related information management laws.

§ 3601. Definitions

The new chapter 36 uses the definitions provided in 44 U.S.C. 3502, but provides eight additional definitions, including:

- *Electronic Government,* which is the use of "web-based Internet applications and other information technologies" to "enhance the access to and delivery of Government information and services" or improve Government operations;
- *Enterprise architecture,* which is defined as strategic information base and described as including a baseline architecture, a target architecture, and a sequencing plan; and
- *Integrated service delivery,* which 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."

§ 3602. Office of Electronic Government

This section establishes an OMB Office of Electronic Government, to be headed by an Administrator for Electronic Government. The E-Gov Administrator's functions are to:

- Assist the OMB Director in carrying out the functions of this Act and other electronic Government initiatives [§ 3602(c)];
- Assist the OMB Director and work with the OIRA Administrator "in setting strategic direction for implementing electronic Government" under the Paperwork Reduction Act (PRA), the Clinger-Cohen Act (subtitle III of title 40 of the U.S. Code), the Privacy Act (section 552a of title 5), the Government Paperwork Elimination Act (GPEA), the Federal Information Security Management Act of 2002, and the Computer Security Act [§ 3602(d)];
- Work with the OIRA Administrator and other OMB offices to oversee implementation of E-Gov under this Act, the PRA, and other laws relating to a variety of information resources management (IRM) functions, e.g., information technology (IT) capital planning and investment control, information security, privacy, and other areas of E-Gov [§ 3602(e)];
- Assist the OMB Director by performing E-Gov functions, as follows:
  1. Advise on resources needed for Federal information systems;
  2. Recommend changes in E-Gov strategies and priorities;
  3. "Provide overall leadership and direction to the executive branch on electronic Government."
  4. "Promote innovative uses of information technology;"
  5. Oversee the E-Gov Fund;
  6. Coordinate with the General Services Administration (GSA) re: GSA E-Gov and IT programs;
  7. "Lead the activities" of the Chief Information Officers (CIO) Council;

8. Assist the OMB Director in establishing policies to support IT standards, developed by the National Institute of Standards and Technology (NIST) and issued by the Secretary of Commerce, including standards for interconnectivity and interoperability, for categorizing Federal electronic information, and for computer system efficiency and security;

9. Sponsor dialogue with governmental and non-governmental leaders to improve IRM and innovative use of IT;

10. Sponsor activities to involve the public in improving "citizen-centered" strategies and services;

11. Oversee the development of the "integrated Internet-based system" by GSA and other agencies;

12. Coordinate with the Administrator for Federal Procurement Policy to ensure effective electronic procurement initiatives;

13. Assist agencies in implementing accessibility standards in the Rehabilitation Act of 1973;

14. Oversee the development of agency enterprise architectures;

15. Assist in overseeing that agency e-Gov activities have adequate security;

16. Administer the Office of Electronic Government; and

17. Assist in preparing the E-Government Report [§ 3602(f)].

§ 3603. Chief Information Officers Council

This section establishes the CIO Council. The Council is comprised of the OMB Deputy Director for Management (DDM), the E-Gov Administrator, the OIRA Administrator, CIO's from major agencies, the CIA, the Department of Defense Service CIO's, and any other Federal employees designated by the DDM. The E-Gov Administrator is to lead the activities of the Council on behalf of the DDM who chairs the Council. GSA is to provide administrative and other support to the Council.

The CIO Council is the principal interagency IRM forum with functions to include:

- Development of recommendations for OMB on IRM policies and requirements;
- Sharing of IRM best practices and innovative approaches;
- Assisting the E-Gov Administrator with multi-agency and other innovative initiatives to improve government performance through the use of IT;
- Promoting common IRM performance measures;
- Helping NIST and the E-Gov Administrator develop recommendations on IT standards
- Working with OPM to improve IRM staffing;
- Working with the Archivist of the U.S. to assess how IRM activities can address Federal Records Act issues; and
- Regular consultation with representatives of State, local, and tribal governments.

§ 3604. E-Government Fund

This section establishes an E-Government Fund in the U.S. Treasury. GSA is to administer the Fund to support projects ap-

proved by the Director of OMB, assisted by the E-Gov Administrator, that improve the ability of the Federal Government to conduct activities electronically using the Internet and other electronic methods. Projects funded by the Fund may include efforts to make information and services more readily available to the public, make it easier for the public to conduct transactions with the Federal Government, and improve information sharing among government agencies.

The E-Gov Administrator is to establish procedures for funding, consult with interagency councils, and assist the OMB Director in coordinating agency expenditure of funds. The E-Gov Administrator is also to adhere to procedures to insure accountability, planning and review, including the OMB Director's final authority to select projects to be funded. Finally, the E-Gov Administrator is to recommend projects for funding based on criteria that include meeting needs of identified groups, ensuring security and privacy, interagency in scope, performance objectives tied to agency mission goals, as well as 12 criteria for ranking proposals that focus on innovative Government-wide applications of information technology.

No Fund money may be transferred to an agency until 15 days after GSA reports to Congress. OMB is to report annually to Congress on the Fund as part of the E-Government report required under § 3606. Authorization of appropriations rises from $45 million in 2003 to $150 million in 2006, with such sums as are necessary authorized for 2007, with all appropriated funds available until expended.

§ 3605. Program to encourage innovative solutions to enhance electronic government services and process

This section, which is based on H.R. 4629, introduced by Representative Tom Davis on May 1, 2002, would provide for a program run by the E-Government Administrator to encourage contractor innovation by the issuance of announcements seeking innovative solutions to enhance electronic government services and processes. The program would include the formation of a multiagency technical assistance team to screen the proposals submitted. After evaluating the proposals the team would submit them, along with the assessment, to the Administrator who would consider funding appropriate proposals under the E-Government Fund or forward them to the appropriate agency.

§ 3606. E-Government report

This section requires the OMB Director to submit an annual E-Government report to Congress. The report is to contain a summary of information reported by agencies (including the E-Gov Status Report required by sec. 202(g)), information about the operations of the E-Gov Fund, and a description of compliance with the Act.

SEC. 102. CONFORMING AMENDMENTS

Sec. 102(a). Electronic Government and information technologies

This subsection amends chapter 3 of title 40, U.S. Code to add a new section 305 to require GSA to consult with the OMB E-Gov office on Electronic Government and other IT initiatives.

Sec. 102(b). Modification of Deputy Director for Management Functions (DDM)

This subsection amends 31 U.S.C. 503(b), which establishes the functions of the OMB DDM, to state that the DDM chairs the CIO Council.

Sec. 102(c). Office of Electronic Government

This subsection amends 31 U.S.C. 505 to state that the E-Gov office is an office of OMB.

TITLE II—FEDERAL MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

SEC. 201. DEFINITIONS

This section states that unless otherwise provided, the title uses definitions from the Paperwork Reduction Act (44 U.S.C. 3502) and title I of the Act.

SEC. 202. FEDERAL AGENCY RESPONSIBILITIES

This section provides a variety of requirements for agencies under the Act.

Sec. 202(a). In general

This subsection requires each agency head to ensure: (1) compliance with the Act, related OMB information resource management (IRM) policies and guidance, and IT standards promulgated by the Commerce Secretary; (2) effective communication of such policies, guidance, and standards to relevant agency officials; and (3) support for OMB and GSA efforts to develop, maintain, and promote an integrated Internet-based system of delivering information and services to the public.

Sec. 202(b). Performance integration

This subsection requires agencies to: (1) develop E-Gov performance measures; (2) try to rely on existing data collections; (3) consider measuring performance in customer service, agency productivity, and use of innovative technology; (4) link their performance goals as appropriate to key groups and to "internal Federal Government operations;' and (5) try to "work collectively in linking their performance goals" to such groups and use IT to deliver information and services to those groups.

Subsection 202(c). Avoiding diminished access

This subsection requires agency heads to consider the impact of E-Gov initiatives on persons without access to the Internet, ensure that the availability of government services and information has not been diminished for such persons, and "pursue alternate modes of delivery" to make such services and information available to them. This provision is complemented by the requirement in sec. 215 for a study of disparities in access to the Internet.

Subsection 202(d). Accessibility to people with disabilities

This subsection states that agencies must comply with section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d).

Subsection 202(e). Sponsored activities

This subsection states that agencies must support the use of IT "to engage the public in the development and implementation of policies and programs."

Subsection 202(f). Chief Information Officers (CIO)

This subsection states that agency CIO's are to participate in the CIO Council and monitor implementation of IT standards.

Subsection 202(g). E-Gov status report

This subsection states that each agency must submit an annual report to OMB on the status of implementation of E-Gov initiatives and compliance with the Act.

Subsection 202(h). Use of technology

This subsection states that nothing in the Act supersedes any agency responsibility "to use or manage information technology to deliver Government information and services that fulfill the statutory mission and programs of the agency."

Subsection (i). National security systems

This subsection states that Title II of the Act does not apply to national security systems, as defined at 40 U.S.C. 11103, except sections 202, 203 and 214 apply to such systems "to the extent practicable and consistent with law."

SEC. 203. COMPATIBILITY OF EXECUTIVE AGENCY METHODS FOR USE AND ACCEPTANCE OF ELECTRONIC SIGNATURES

This section supports the interoperable implementation of electronic signatures that are necessary for secure electronic transactions with Government. The section requires agencies to ensure that their methods for the use and acceptance of electronic signatures are compatible with OMB policies and procedures. The section also requires GSA to establish a framework for efficient interoperability among agencies when using electronic signatures, including digital signatures. To support this effort, the section authorizes the appropriation of $8 million in FY 2003 and such sums as necessary for each year thereafter for a Federal bridge certification authority to support interoperable use of digital signatures and for other electronic signature initiatives.

SEC. 204. FEDERAL INTERNET PORTAL

This section directs the Director of OMB to work with GSA and other agencies to "maintain and promote" an integrated Internet-based system to give the public consolidated access to Government information and services (State and local, as well as Federal) from a single point, and organized according to function rather than agency jurisdiction. The section further authorizes to be appropriated to GSA $15,000,000 for the system for fiscal year 2003 and such sums as necessary for fiscal years 2004–2007.

SEC. 205. FEDERAL COURTS

This section requires the Supreme Court, each circuit court, each district court, and each bankruptcy court of a district to establish

a website for public access to current and updated information about the court and cases before the court, including electronic filings. The section does, however, permit courts to defer compliance if they notify the Administrative Office of the U.S. Courts of the reasons for the deferral. The Judicial Conference of the U.S. is to report to Congressional Committees on the deferral notifications. The section is intended to provide the public with greater access to judicial information.

SEC. 206. REGULATORY AGENCIES

This section requires Federal agencies to improve public online access to agency information. To the extent practicable, and in consultation with the Office of Management and Budget, agencies are to: (1) Include in a publicly accessible website all information required to be published in the Federal Register under the Freedom of Information Act, at 5 U.S.C. 552(a)(1) & (2); (2) Accept public rulemaking comments by electronic means; and (3) Have a public website containing electronic rulemaking dockets, including public comments and other material in the agency's rulemaking docket.

SEC. 207. ACCESSIBILITY, USABILITY, AND PRESERVATION OF GOVERNMENT INFORMATION

This section would improve the organization, preservation, and public accessibility of Government information, including information on the Internet.

First, OMB is to establish the Interagency Committee on Government Information to consult with interested parties, conduct studies, submit recommendations, and share effective practices with regard to information access, dissemination and retention. On the basis of recommendations from that committee, OMB is to issue policies on: (1) Standards for the organization and categorization of Government information in ways that are searchable electronically and are interoperable across agencies; (2) Categories of Government information to be classified under the standards; and (3) Priorities and schedules for the initial agency implementation of the standards.

Also on the basis of recommendations of the committee, the National Archives and Records Administration (NARA) is to issue policies and procedures to ensure that Federal Records Act (chapters 21, 25, 27, 29, and 31 of title 44, U.S. Code) requirements are applied to Government information on the Internet and to other electronic records.

The section requires OMB to issue guidance for agency websites with requirements for links to descriptions of an agency's organization, mission and statutory authority, as well as public information under the Freedom of Information Act (5 U.S.C. 552(a)(1) and (b)). The OMB guidance is also to include minimum goals for agencies to assist public users to navigate agency websites, e.g., search retrieval speed, data aggregation tools, and security protocols.

Agencies are to consult with the committee and the public as part of establishing 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.

The section also requires the establishment of a public domain directory of public Federal Government websites that is to be devel-

oped in a collaborative effort with librarians, IT managers, records managers, and others.

The section, at subsection (g), also requires the OMB Director to work with the Office of Science and Technology Policy (OSTP) and other agencies to ensure the development and maintenance of a repository, and one or more publicly accessible websites, with detailed information about federally funded research and development (R&D). OMB is to issue guidance for the information to be put in the repository. The repository and website(s) are to include information about: (1) Federally funded R&D performed by the Federal Government and institutions and individuals outside the Federal Government; and (2) Each separate R&D task or award, including dates, summaries, objectives, researchers, funds, information restrictions, and other information.

The purpose of creating broader access to this information is to facilitate: coordination of Federal R&D, collaboration among researchers; technology transfer; and access by policymakers and the public to information about Federal R&D. The subsection would authorize to be appropriated $2 million in each of fiscal years 2003–2005.

SEC. 208. PRIVACY PROVISIONS

This section requires agencies, with OMB guidance, to conduct and review a privacy impact assessment before collecting information in an identifiable form, or developing or procuring information technology that collects, maintains, or disseminates such information. The definition of information in an "identifiable form" means information that permits the identity of the individual to whom the information applies to be reasonably inferred directly or indirectly.

This section also requires OMB to issue guidance for privacy notices on agency public websites. The notices are to address what and why information is collected, its use, with whom it will be shared, individual rights with regard to the information, and how the information will be secured. The OMB guidance is also to address translating privacy policies into standardized machine-readable formats.

SEC. 209. FEDERAL INFORMATION TECHNOLOGY WORKFORCE DEVELOPMENT

This section requires the Office of Personnel Management (OPM) in consultation with OMB, the CIO Council, and GSA, to analyze Federal IT and IRM personnel needs, oversee the development of training programs, and assess the adequacy of training for Federal employees in IT "disciplines." In carrying out these duties, the Director of OPM may provide for a program allowing federal workers to be detailed to the private sector for training purposes, under section 3703 below.

The section at subsection (c) would also amend subpart B of part III of title 5 of the U.S. Code by adding a new chapter 37 establishing an IT exchange program. The provisions are also contained in legislation previously introduced as H.R. 3925, the Digital Tech Corps Act of 2002, which was reported by the Government Reform Committee on March 14, 2002, and passed the House of Representatives on April 10, 2002. The provisions of the new chapter 37 are as follows:

§ 3701. Definitions

For purposes of this chapter, the term "agency" applies only to executive branch agencies, and the term "detail" means either an assignment of an employee of a private sector company to a Federal agency, or it means an assignment of an employee of a Federal agency to a private sector company.

§ 3702. General provisions

a. *Initiation and Eligibility provisions:* The IT Exchange Program is initiated via an agreement of the agency, the private sector organization, and the employee involved. Eligible employees are those that are: (1) working in IT management; (2) considered exceptional performers; and (3) expected to assume increased IT management responsibilities in the future. Employees detailed from the Federal government must be in the GS 11–15 range and serving under career or career-conditional appointment (or the equivalent in the excepted service). Schedule C employees are prohibited from participation.

b. *Written agreement required:* Establishing an IT Exchange Program requires a written agreement between the agency, the employee and the private sector organization involved. This agreement must contain, at a minimum, requirements that Federal employees must return to service of the Government for a period of not less than the length of the exchange (on penalty of paying the Government back the costs of the exchange).

c. *Assignment Termination:* Provides that the agency or the private sector organization involved can terminate the exchange program at any time, for any reason.

d. *Duration of Exchange:* Provides that exchange assignments under this program will be from three months to 1 year and can be extended in 3 month increments for up to one additional year (i.e., 2 year maximum).

e. *Chief Information Officers Council Participation:* Provides that the CIO Council may participate in the administration of the IT Exchange Program.

f. *Small Business Concerns:* Requires that small business concerns be appropriately represented in the IT Exchange Program.

§ 3703. Assignment of employees to private sector organizations

a. *Detail of a Regular Work Assignment:* This clarifies that a Federal employee who agrees to participate in the IT Exchange Program remains a Federal employee while detailed to a private sector organization. Thus she or he will retain uninterrupted pay, credits for step increases, retention, sick and leave accrual, insurance, and retirement benefits. Nothing about participation in the IT Exchange Program will be detrimental to the Federal employee's career, livelihood, or benefits.

b. *Coverage Under Workers Compensation and Wrongful Death:* This provision specifies that while on detail, a Federal employee retains his or her coverage for purposes of injury or death while on the job. Also, so that there is no double compensation, the provision also states that if the Federal employee is similarly covered by the private sector organizations, the payment or benefit for the same injury or death will be appropriately credited.

c. *Travel and Transportation Cost Reimbursements:* This provision allows agencies to fund the travel and transportation costs of Federal employees participating in the IT Exchange Program. This reimbursement is subject to the same conditions as are applicable in 5 U.S.C. § 3375.

d. *Tort Claims Act Protection:* This provision provides that a Federal employee assigned to a private sector organization under the IT Exchange Program is covered under the Federal Tort Claims Act and any other Federal tort liability statutes.

e. *Small Business Concerns:* Requires that agencies ensure that 20% of assignments in the IT Exchange Program are to small business concerns as defined in the Small Business Act.

§ 3704. Assignment of employees from private sector organizations

a. *In General:* This provision provides that an employee of a private sector organization assigned to an agency under this chapter is deemed to be on detail to such agency. The purpose of this section is to provide that a private sector employee's pay and benefits are to be provided by the private sector employer while on the detail. There is no cost to the government for this employee's services while detailed.

b. *Terms and Conditions:* An employee of a private sector organization assigned to an agency under this chapter is governed by the following four provisions.

1. The employee may receive pay from the private sector employer: This provision clarifies that a private sector employee will not be in violation of ethics statutes for receiving pay from the employee's private sector employer under the IT Exchange Program.

2. The employee is deemed a Federal government employee for purposes of Federal employee ethics and revolving door requirements, including:

A. Chapter 73 of title 5 of the U.S. Code: This puts a Tech Corps private sector participant who is detailed to a Federal agency under the provisions of the Hatch Act, except that the salary received from the private sector employer is not considered an impermissible act;

B. Sections 201, 203, 205, 207, 208, 209, 603, 606, 607, 643, 654, 1905, and 1913 of title 18 of the U.S. Code: These criminal law provisions govern the behavior of private sector Tech Corps participants while detailed to agencies. They include restrictions and prohibitions against:

- Acting as a lobbyist (1 year after detail);
- Accepting bribes for official work;
- Aiding in the obtaining of contracts (1 year after detail);
- Suing the government (other than in the proper discharge of official duties);
- Revolving door activities;
- Financial conflicts of interest;
- Making political contributions;
- Intimidation to secure political contributions;
- Receipt of political contributions;
- Embezzlement;
- Disclosure of confidential information/trade secrets during and for 3 years after detail; and

• Lobbying with appropriated funds;

C. Sections 1343, 1344, and 1349(b) of title 31 of the U.S. Code: These provisions state that Tech Corps detailees are forbidden to have government funded cars or planes;

D. The Federal Tort Claims Act and any other Federal tort liability statute;

E. Ethics in Government Act of 1978;

F. Section 1043 of the Internal Revenue Code of 1986: This provision affects sale of property to resolve financial conflicts of interest and specifies how the IRS treats these sales; and

G. Section 27 of the Office of Federal Procurement Policy Act: This provision would prohibit Tech Corps detailees from disclosing procurement information, during and for 3 years after the detail.

3. The employee 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.

4. The employee is subject to such regulations as the President may prescribe to govern the IT Exchange Program.

In addition, private sector employees working at Federal agencies will be under the supervision of the agency's Federal managers.

c. *Private Sector Employee Covered by Workers Compensation and Wrongful Death If Not Otherwise Covered:* This provision provides that if a private sector employee participating in the IT Exchange Program is not covered by a private sector company for workers compensation or wrongful death, then the Government will provide these benefits if injury or death occurs during the performance of official duties under the IT Exchange Program.

d. *Prohibition on Charging Costs:* This provision prevents private sector company with an employee on assignment to the IT Exchange Program from charging the costs of pay or benefits under a Federal Government contract.

§ 3705. Application to Office of the Chief Technology Officer of the District of Columbia

This section provides that the Tech Corps program applies to IT workers in the District of Columbia government.

§ 3706. Reporting requirement

This section requires OPM to do a semiannual report to congressional committees summarizing the operation of this chapter.

§ 3707. Regulations

This section provides that OPM is to issue regulations implementing the IT Exchange Program. It also requires that OPM prepare a report identifying all existing exchange programs and IT training opportunities for Federal employees. Also requires that the General Accounting Office (GAO) report on the IT Exchange Program established in this chapter not later than four years after enactment (program sunsets in five years). Finally the section provides for a number of technical and conforming amendments to current law, including titles 5, 18, and 31 of the U.S. Code.

SEC. 210. SHARE-IN-SAVINGS INITIATIVES

The section would amend chapter 137 of title 10, U.S. Code and title III of the Federal Property and Administrative Services Act to authorize government-wide the use of share in savings contracts for information technology. These contracts represent an innovative approach to encourage industry to share creative technology solutions with the Government. Through these contracts agencies can lower their costs and improve service delivery without large "up front" investments as the contractor provides the technology and is compensated by receiving a portion of savings achieved. The section is based upon a provision contained in the Services Acquisition Reform Act of 2002, H.R. 3832.

The section would authorize agencies to enter into share-in-savings contracts for information technology for a term of 5 years, and with the appropriate approval for up to 10 years, to pay contractors from the savings realized, and to retain those savings that exceed the amount paid to the contractor. The section would permit agencies to use various options for funding cancellation or termination costs and would permit the cancellation or termination amount to be negotiated by the parties. The section would require that contracts awarded pursuant to this section include a provision containing a quantifiable baseline for savings that is approved by the agency's senior procurement executive. Currently, agencies subject to title 10 of the U.S. Code would be permitted to enter into an aggregate of up to 5 contracts each during fiscal years 2003, 2004, and 2005 where funds are only available for the first fiscal year of the contract and certain conditions met. The same number would be authorized for the same period for agencies under title 41 of the U.S. Code. The number of such contracts authorized would increase to an aggregate of ten for agencies under each title starting in 2006. Further, the section would require that the Federal Acquisition Regulation (FAR) be revised to implement this section and to provide for such matters as the use of competitive procedures and innovative provisions for technology refreshment, appropriate regulatory flexibility to facilitate the use of such contracts. Further, GSA is to provide additional guidance to agencies in identifying additional opportunities for the use of these contracts and for determining baselines and saving share ratios. Finally, the section would require the Director of OMB to report to Congress two years after enactment describing the number of share-in savings contracts entered into and making recommendations for changes in law needed to encourage their use and the GAO would review the OMB report. The provisions would sunset in September 2009.

SEC. 211. AUTHORIZATION FOR ACQUISITION OF INFORMATION TECHNOLOGY BY STATE AND LOCAL GOVERNMENTS THROUGH FEDERAL SUPPLY SCHEDULES

The section would amend section 502 of title 40 of the U.S. Code to give the GSA Administrator the authority to provide for the use by State or local governments of the Federal Supply Schedules of the GSA for automated data processing equipment, software, support equipment and services, and other items contained in Federal supply classification group 70. The section would further provide that participation by a Federal Supply Schedule contractor in a

sale to a State or local government would be voluntary. Not later than December 31, 2004, the Administrator is to report on the implementation and effects of the new provision.

SEC. 212. INTEGRATED REPORTING STUDY AND PILOT PROJECTS

This section would enhance the interoperability of Federal information systems; reduce information collection burdens and assure accuracy of submitted information; and enable individuals to integrate and obtain similar bodies of agency information.

The section requires the OMB to report to Congress within 3 years on progress toward integrating Federal information systems across agencies. The report is to address:

- The integration of data elements used in electronic information collection within Federal databases "established under Federal statute;"
- The feasibility of developing software "for use by reporting persons in assembling, documenting, and validating the accuracy of information electronically submitted to agencies under non-voluntary, statutory, and regulatory requirements;"
- The feasibility of developing a distributed information system involving at least 2 agencies to allow the integration of public information held by the agencies and provide public access "to the information holdings of 1 or more agencies, or some portion of such holdings, including the underlying raw data, without requiring public users to know which agency holds the information".

To assist in the study, OMB is designating up to 5 pilot projects to integrate data elements in order to reduce information collection burdens by eliminating duplicative data, create interoperability among public databases, and use software to reduce errors.

SEC. 213. COMMUNITY TECHNOLOGY CENTERS

This section requires a study by the E-Gov. Administrator of best practices of Federally funded community technology centers, how to enhance their development, and how to improve sharing of information and resources. The E-Gov. Administrator in consultation with the Secretary of Education is to work with other agencies to assist in the implementation of the study's recommendations. The E-Gov. Administrator in consultation with the Secretary of Education is also to develop an online tutorial to explain how to access Government information and services on the Internet.

SEC. 214. ENHANCING CRISIS MANAGEMENT THROUGH ADVANCED INFORMATION TECHNOLOGY

This section provides for a 2-year study to be performed by a contractor and overseen by the E-Gov. Administrator in consultation with the Federal Emergency Management Agency (FEMA), to develop a research and implementation strategy for the use of IT in disaster preparedness, response, and recovery. Based on the results of the study, the E-Gov. Administrator in consultation with FEMA is to initiate pilot projects or report to Congress on other activities to maximize the use of IT in disaster management.

SEC. 215. DISPARITIES IN ACCESS TO THE INTERNET

This section provides for a 2-year study to be requested by GSA and conducted by a contractor selected by the National Academy of Sciences on disparities in Internet access for online government services. The study is to include recommendations for ensuring that online government initiatives do not have the "unintended result of increasing any deficiency in public access to Government services."

TITLE III—INFORMATION SECURITY

Title III contains six sections:

- Section 301 revises GISRA, the Government Information Security Reform provisions of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001 (Div. A, Title X, Subtitle G, sec. 1061–1065; Pub. L. 106–398, October 30, 2000), and is drafted as a substitute to subchapter II of chapter 35 of title 44, U.S. Code, to facilitate understanding given the number of amended provisions;
- Section 302 amends the Federal information systems standards provisions of the Clinger-Cohen Act regarding promulgation of NIST-developed information security standards (40 U.S.C. 11331, originally enacted into law as sec. 4 of the Computer Security Act of 1987);
- Section 303 revises NIST's information security and systems standards role (15 U.S.C. 278g–3, section 3 of the Computer Security Act);
- Section 304 revises the role of the NIST Computer System Security and Privacy Advisory Board (15 U.S.C. 278g–4, section 3 of the Computer Security Act);
- Section 305 makes technical and conforming amendments, including repealing unnecessary provisions of the Computer Security Act and the Paperwork Reduction Act;
- Section 306 provides rules of construction to ensure proper implementation of standards promulgation authority by OMB and the Department of Commerce.

SEC. 301. INFORMATION SECURITY

Subsection (a) states that this title may be cited as the "Federal Information Security Management Act of 2002" (FISMA), reflecting its origins in H.R. 3844, of the same name.

Subsection (b) amends subchapter II of chapter 35 of title 44, U.S. Code, to include the following provisions.

§ 3531. Purposes

The provision provides that the purposes of this subchapter are to:

- Provide a comprehensive framework for ensuring the effectiveness of Federal information security through a risk-based entity-wide management approach;
- Recognize the highly networked nature of the Federal computing environment and provide effective government-wide management and oversight of related information security risks;
- Provide for the development and maintenance of minimum security controls;

- Provide a mechanism for improved oversight through annual independent evaluations of agency information security practices;
- Acknowledge that commercial available information security products offer effective information solutions; and
- Recognize that the selection of specific technical information security solutions should be left to individual agencies from among commercially developed products.

§ 3532. Definitions

The definition for the term "information security" covers the protection of both information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. This definition addresses the three objectives of information integrity, confidentiality, and availability. These three concepts are the widely accepted key organizing principles for information security and encompass concepts such as non-repudiation and authenticity. Including the three objectives reflects the importance of recognizing that information security not only involves keeping secrets (confidentiality), but also depends on protecting the ability to use and rely on information and information systems (integrity and availability).

This section's definition of "national security system" encompasses the longstanding statutory treatment of military and intelligence mission-related systems and classified systems. This definition replaces Government Information Security Reform Act's (GISRA) introduction of the term "mission critical system." It restores reliance on: (1) "Warner Amendment" national security systems, most recently reenacted into law in section 5142 of the Clinger-Cohen Act of 1996, at 40 U.S.C. 11103(a); and (2) the Computer Security Act's treatment of systems protected by procedures for information authorized to be kept secret in the interest of national defense or foreign policy, at 15 U.S.C. 278g–3. The provision uses "classified" instead of "secret" to reflect the use of the term in recent Executive Orders on information classification.

This section's definition of "information technology" references the current definition of the term in the Clinger-Cohen Act, at 40 U.S.C. 11101(6).

§ 3533. Authority and functions of the Director

This section states that OMB is to oversee agency information security policies and practices, including through:

1. Developing and overseeing information security policies, principles, standards and guidelines, including through the promulgation of standards and guidelines developed by NIST;
2. Requiring agencies to identify and provide information security protections commensurate with the risk and the magnitude of harm to information and information systems;
3. Coordinating the development of NIST standards with agencies responsible for national security systems to ensure that NIST-developed standards and national security system standards are complementary;
4. Overseeing agency compliance with the requirements of this Act, including through authorized action, such as through

the budget process, to enforce agency accountability for compliance with this subchapter;

5. Annually reviewing, and approving or disapproving, agency information security programs;

6. Coordinating information security policies and procedures with related IRM policies and procedures;

7. Overseeing the Federal information security incident center, required under § 3536; and

8. Reporting to Congress on agency compliance with the subchapter.

The purpose of these provisions is to clarify and streamline OMB's statutory requirements in comparison with those under GISRA. The new section eliminates unnecessary and redundant language and harmonizes the provisions with current law in the Paperwork Reduction Act and the Clinger-Cohen Act. It also strengthens OMB's role in several respects, for example, heightening its responsibility to ensure agency compliance with information system and security standards.

This section also clarifies the scope of the law with regard to the treatment of national security systems. At § 3533(b), it provides that OMB's authorities under this section do not apply to national security systems except for oversight of agency compliance under subsection (a)(4), and reporting to Congress under subsection (a)(8). The purpose of this provision is to recognize OMB's continuing oversight and reporting responsibilities, while also recognizing that information security for national security systems is to be provided under standards and guidelines as required by law and as directed by the President for national security systems. Neither NIST nor OMB will establish requirements for those systems. This mandate is reiterated in the statement of general agency responsibilities, at § 3534(a)(1)(B), and in a separate section specifically on agency responsibilities for national security systems, at § 3537. This approach is consistent with that of Executive Order No. 13231 (October 16, 2001).

§ 3534. Federal agency responsibilities

This section details Federal agency information security responsibilities:

1. Agency heads are responsible for agency information security;

2. Senior program officials are responsible for applying the risk-based approach to securing the information and systems supporting the operations and assets under their control;

3. The agency CIO is responsible for ensuring agency compliance with the subchapter's requirements;

4. Each agency must have an agency-wide information security program; and

5. Each agency must report on its information security activities in budget and management reports.

This section maintains the key requirements in GISRA for agencies to establish agency-wide information security programs. FISMA goes on, however, to revise the GISRA provisions in this section to streamline provisions and more clearly specify key agency requirements.

First, § 3534(a)(1)(B), provides that agencies must comply with NIST-developed information security standards, as well as applicable national security system standards. This provision bases agency information security programs in compliance with standards, as well as in individual agency risk management. Historically, Federal information security system standards have not been mandatory. Agencies will be responsible for compliance with all applicable standards—for national security as well as non-national security systems. While standards development and oversight is divided between NIST and OMB for non-national security systems and the Department of Defense (including roles for the Director of Central Intelligence and the National Security Agency) for national security systems, it remains the obligation of every agency to comply with applicable requirements to provide adequate security for information and information systems supporting the agency's operations and assets, whether they involve non-national security or national security systems. While some agencies may have only one or the other, others have both national security and non-national security systems. The key to information security for those agencies is to have an agency-wide information security program that can address both national security and non-national security system security needs, including compliance with applicable standards.

Third, § 3534(a)(3) describes the information security responsibilities of each agency CIO. This expands the same subsection in GISRA to include a more detailed requirement for the designation of a senior agency information security officer. Under this provision, this official is to: (1) carry out the CIO's responsibilities under the Act; (2) possess appropriate professional qualifications; (3) have information security as his or her primary duty; and (4) head an information security office with the mission and resources needed to help ensure agency compliance with the Act. GAO has found that an information security best practice is the establishment of a central management focal point to ensure adequate attention to information security. This provision will help agencies implement this practice.

Fourth, § 3534(b) requires each agency to "document" its agency-wide security program, and prepare "subordinate plans" as needed for networks, facilities, and systems, at § 3534(b)(3). These provisions replace GISRA's alternating use of "program" and "plan," as well as the Computer Security Act's exclusive reliance on individual system security plans, repealed at sec. 305(a). These provisions are meant to ensure that each agency's information security program will represent an agency-wide management process that is adequately documented at appropriate component and agency-wide levels.

Fifth, § 3534(b)(5) strengthens GISRA by providing more precise management testing and evaluation requirements. Each agency information security program must include periodic testing and evaluation of the effectiveness of policies, procedures, and practices, to be performed. depending on risk, but at least annually. This requirement is part of the ongoing obligation of systems owners and managers to maintain a current understanding of the security status of their systems and the steps needed to address security weaknesses.

This requirement is not intended to mean the degree of testing and evaluation associated with formal certification and accreditation (C & A) processes, although timely C & A testing, as well as other relevant tests and evaluations, can be used to satisfy this requirement. Rather, it reflects the need for program officials and systems owners to maintain an understanding of the effectiveness of the security controls for programs and systems over which they have responsibility. Overall, this provision underscores the need for periodic control checks as a matter of ongoing management responsibility. Particularly given the rapid pace of emerging threats and vulnerabilities, waiting as much as three years for a formal C & A will not provide an adequate assurance that appropriate controls are in place and operating as intended.

Finally, § 3534 refines a number of GISRA provisions with regards to agency information security responsibilities:

- The section adds a paragraph, at § 3534(b)(8), to require agencies to have plans and procedures to ensure continuity of operations. Public and private sector experience with hackers and viruses has proven the absolute necessity for agencies to have contingency plans to help restore critical systems and applications after disruptions to agency operations.
- The section strengthens oversight of agency information security activities with a requirement at § 3534(c)(1) for agencies to report annually to OMB, GAO, and Congress. This replaces the GISRA provision that provides that each agency security program be "subject to the approval" of the OMB Director, at 44 U.S.C. 3534(b)(3). It should be noted that the annual reporting requirement is not intended to lead to multiple duplicative reports. OMB guidance should facilitate the combination of any similar reports as long as the resulting report addresses the requirements of this Act. Thus, for example, the Department of Defense should, with OMB guidance, ensure that its annual report satisfies the requirements of both this Act and the Defense Information Assurance Program (DIAP) under 10 U.S.C. 2224.
- The section clarifies that any significant information security deficiency be reported as a material weakness in reporting under 31 U.S.C. 3512 (the Federal Managers Financial Integrity Act), and, if relating to financial management systems, as an instance of a lack of substantial compliance under 31 U.S.C. 3512 note (the Federal Financial Management Improvement Act), at § 3805(c)(3).
- The section adds a provision, at § 3534(e), to require agencies to give public notice and opportunity to comment on proposed information security policies and procedures that affect communication with the public, such as encryption standards. This requirement should not be interpreted as requiring disclosure of information security procedures and practices that would reveal vulnerabilities or otherwise increase information security risks.

§ 3535. Annual independent evaluation

This section requires that each agency have performed an annual independent evaluation of its information security program and practices by either its Inspector General or an independent exter-

nal auditor. The evaluation is to be submitted to the OMB Director, who is to summarize the results in the annual report to Congress on compliance with the subchapter.

This section continues the GISRA requirement for an annual independent evaluation at 44 U.S.C. 3535. Several changes are made to the provisions of the section for the sake of clarity. For example, § 3535(a)(2)(A) is revised by substituting "representative" for "appropriate." An evaluation should involve the examination of a sample of systems and procedures. Such a sample should be representative of the whole. The word "appropriate" does not express that concept. The word "representative" also better reflects the Committee's view that the evaluations are meant to provide an overview of each agency's information security program and practices, rather than an exhaustive review of every system and procedure.

The section is revised to clarify procedures for evaluating national security systems within the context of the agency-wide evaluation. These revisions address the confusion created when GISRA established separate procedures for the evaluation of national security systems and left unexplained the relation of those evaluations to the agency-wide evaluation. Because most agencies with national security systems also have non-national security systems, agency-wide evaluations must take into account both categories of systems.

To achieve this goal of a more reasoned approach to the evaluation of agency-wide information security, including national security systems, this section provides that:

- Agencies and evaluators must take appropriate steps to protect information, which, if disclosed, might harm information security—this provision, at § 3535(f), preserves the GISRA provisions, at 44 U.S.C. 3535(e), regarding the responsibility of agencies and their evaluators to take all necessary precautions to protect security while performing the required evaluations.
- The evaluations should have separate presentations, as appropriate, regarding information security for national security systems—this new formulation, at § 3535(a)(2)(C), ensures that while all necessary steps are taken to protect the security of national security systems, the agency will have a record of a comprehensive evaluation of its information security program and practices.
- The portion of the agency-wide evaluation directly relating to a national security system shall be performed by an evaluator chosen by the agency and in such a manner to ensure appropriate information security protections—this subsection, at § 3535(c), preserves the GISRA provision protecting agency responsibility for national security system information security, but revises GISRA, at 44 U.S.C. 3535(b)(1)(B), to ensure that national security system evaluations are performed in the context of the agency-wide evaluation.
- The results of the evaluations shall be submitted to OMB, which will then prepare a summary report for Congress. These provisions, at § 3535(e) and (g) (1) and (2), which revise GISRA at 44 U.S.C. 3535(c) and (d)(1), ensure reporting to OMB and Congress, while protecting information security by requiring submission to OMB of the evaluation results, not the evaluation itself, and requiring reporting to Congress on a summary

of the results, not the results or the evaluations themselves. Furthermore, § 3535(e)(2) specifies that the results of evaluations that directly relate to a national security system should only be submitted to OMB in the form of a summary and assessment. This is meant to ensure that no unnecessary risks are undertaken with regard to national security information through, for example, the burdensome transmission of classified materials to the offices of OMB.

- As under GISRA at 44 U.S.C. 3535(d)(2), evaluations and any descriptions of intelligence-related national security systems shall only be made available to Congress through the Intelligence Committees, at § 3535(g)(3).

Given these FISMA provisions relating to the evaluation of national security systems, the Committee would eliminate the GISRA requirement for audits of evaluations of national security systems at 44 U.S.C. 3535(b)(1)(A), (c)(2), and (d)(2). The Committee believes the GISRA audit of evaluations requirement is unnecessary and unduly complicated.

Finally, § 3535(h) requires periodic GAO evaluation of agency information security policies and practices. This is a new subsection and is meant to ensure that GAO continues to perform its valuable service in assisting Congress in the oversight of Federal information security.

§ 3536. Federal information security incident center

This section directs OMB to ensure the operation of a central Federal information security incident center. The Committee recognizes the current successful operation of GSA's incident center, FedCIRC. The purpose of the requirement in this section is to provide a permanent authorization for a center such as FedCIRC, and to insure that its activities are broadly conceived and faithfully carried out consistent with the mandate in this section. Under subsection (a), the center's mission is to: (1) Provide timely technical assistance to agencies and other operators of Federal information systems; (2) Compile and analyze information security incident information; Inform agencies about information security threats and vulnerabilities; and (3) Consult with national security agencies and other appropriate agencies, e.g., an infrastructure protection office.

The section, at § 3536(b), provides that agencies responsible for national security systems are to share information about information security incidents with the center to the extent consistent with national security system standards and guidelines. This provision is intended to encourage inter-agency communication and consultation, while preserving national security agency discretion to determine appropriate information sharing.

§ 3537. National security systems

This section states that agencies operating or controlling national security systems must: Provide information security protections commensurate with the risk and magnitude of harm for information maintained in such systems; Implement all applicable national security system standards and guidelines; and Comply with the requirements of the subchapter.

The purpose of the section is to make clear that agencies must manage national security systems consistent with applicable na-

tional security requirements (independent of OMB or NIST-developed guidance for other systems), but that they must also secure those systems with the same risk-based management approach and the same commitment to agency accountability applicable to all Federal agencies, most notably the requirements at §3534 and § 3535.

§ 3538. Authorization of appropriations

This section authorizes such sums as may be necessary to carry out the provisions of the subchapter for five years. This limited authorization will help ensure periodic congressional oversight, without limiting the effectiveness of the law, as was accomplished by GISRA's two-year sunset, currently at 44 U.S.C. 3536.

§ 3539. Effect on existing law

This section provides that nothing in this subchapter or those provisions of law relating to the development and promulgation of NIST-developed standards may be construed as affecting current authorities regarding the use or disclosure of information, including under the Privacy Act, Freedom of Information Act, the Federal Records Act, the Paperwork Reduction Act, or disclosure of information to the General Accounting Office.

SEC. 301(C). INFORMATION SECURITY RESPONSIBILITIES OF CERTAIN AGENCIES

This subsection states that nothing in this subchapter supersedes any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems. This subsection, at paragraph (B), also amends several provisions of law to clarify and harmonize language with the subchapter. Further, this subsection provides (in the same terms as in GISRA) that nothing in the subchapter supersedes any requirement made by or under the Atomic Energy Act of 1954. Finally, this subsection revises section 1062 of GISRA to eliminate unnecessary statutory language and rely instead on current guidance in OMB Circular A–130, and to simplify the treatment of national security systems.

SEC. 302. MANAGEMENT OF INFORMATION TECHNOLOGY

This section amends 40 U.S.C. 11331 (sec. 5131 of the Clinger-Cohen Act) to:

- Require OMB to issue NIST-developed information security standards, while preserving Commerce promulgation of other information system standards;
- Require that the security standards include minimum mandatory requirements geared to control objectives and risk levels;
- Distinguish between NIST-developed standards and those developed for national security systems; and
- Eliminate the ability to waive standards.

The purpose of this section is to strengthen the process for the promulgation of information security standards.

The section, at subparagraph (a)(1)(A), requires OMB to issue Federal information security standards developed by NIST under

section 20(a)(3) of the NIST Act. This responsibility is limited by paragraph (a)(2), which states the standards and guidelines for national security systems are to be developed, promulgated, enforced, and overseen as otherwise authorized by law and as directed by the President. Thus, this section continues the principle in law since the enactment of the Computer Security Act of 1987, namely that NIST is to develop standards for all Federal systems, other than national security systems.

Under subparagraph (a)(1)(B), OMB must make these standards compulsory to the extent they: (1) Provide minimum mandatory requirements as determined under the NIST Act; or (2) Otherwise are necessary for information security. This requirement for the issuance of minimum mandatory standards is the counterpart to FISMA's other requirements for NIST to develop minimum mandatory standards, and for agency compliance with, and OMB oversight of, such standards (see discussion of sec. 303, below, and 44 U.S.C. 3533 & 3534, above).

Paragraph (a)(3) preserves the provision in current law (at 40 U.S.C. 11331(c)) permitting agencies to use more stringent standards than provided by NIST-developed standards, but only if those more stringent standards incorporate applicable mandatory NIST requirements and are otherwise consistent with the risk management policies and guidelines issued by OMB under 44 U.S.C. 3533. This provision is consistent with the principle that NIST-developed standards are generally intended to provide minimum guidance. The requirements are to be geared to risk levels and would have minimum requirements by such risk levels.

These FISMA provisions permitting the use of more stringent standards should be distinguished from requirements in GISRA to develop "more stringent" policies for national security systems (GISRA, sec. 1062(b)), and to make such policies available to other agencies (GISRA, sec. 1062(f)). The FISMA provisions permit the use of more stringent requirements and envision building more stringent protections on top of minimum requirements, depending on the nature of information security risks. GISRA, on the other hand, mandates the use of requirements for defense systems that provide more stringent protection than that otherwise provided under GISRA (GISRA, sec. 1062(b)). This approach imposes an arbitrary and illogical ceiling on the law's own risk management principles, and could lead to unnecessarily inconsistent approaches to information security.

FISMA eliminates the current provision at 40 U.S.C. 11331(d) permitting waivers of standards. Agencies currently operate under a blanket delegation of waiver authority from the Secretary of Commerce (Memorandum to the Heads of Executive Departments and Agencies, Secretary of Commerce, November 14, 1988). The Committee believes it is inconsistent with the purpose of developing standards needed for information security to provide such a broad waiver under the argument that compliance with the standards would have an adverse impact on the mission of the agency. The fundamental purpose of FISMA is to require each agency to employ information security policies and practices in order to manage risks to the agency's operations and assets. FISMA's equally fundamental presumption is that the Federal government must have a consistent information security approach across all agencies.

FISMA's standards are intended to provide that consistent approach, while meeting the mission-specific needs of each agency. Accordingly, the Committee believes that a strengthened process is needed to focus on developing and implementing workable mandatory standards.

Subsection (b) provides a similarly revised standards promulgation process for the Secretary of Commerce, with regard to systems standards, developed by NIST under section 20(a)(2) of the NIST Act. Again, this process is currently found at 40 U.S.C. 11331.

SEC. 303. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

This section revises section 20 of the National Institute of Standards and Technology (NIST) Act (15 U.S.C. 278g–3), originally enacted as part of the Computer Security Act of 1987, to update the mission of NIST in light of current understandings of information security and related provisions in FISMA.

Subsection (a) maintains NIST's three-part standards mission of developing standards and guidelines for information systems, for Federal information systems, and for Federal information security. However, it updates original Computer Security Act language to focus on information systems and information security, and otherwise conform to the definitions provided in FISMA.

Subsection (b) establishes new requirements for NIST-developed standards to include: (1) Standards for categorizing the criticality and sensitivity of agency information according to information security control objectives and across a range of risk levels, and (2) Minimum information security requirements for each information category. The subsection also would have NIST develop guidance, in coordination with NSA, for identifying national security systems. This guidance is not to govern such systems, but rather to ensure that agencies receive consistent guidance on the identification of systems that should be governed by national security system requirements. NIST is required to develop this guidance in coordination with NSA to ensure consistency with national security system requirements.

Subsection (c) requires NIST to consult with other agencies to improve security and avoid duplication of effort, and to ensure that NIST standards are complementary with national security system requirements. This provision maintains the basic consultation requirements of the Computer Security Act at 15 U.S.C. 278g–3(b)(5) and (c), while revising the language for clarity and consistency with other FISMA terms and requirements. For example, it strikes the reference to achieving consistency "to the maximum extent possible" with national security system requirements, and substitutes a requirement that the NIST-developed standards should be "complementary with standards and guidelines" for national security systems. The use of the term "consistency" has proven unsatisfactory, as it has raised arguments that these standards might be "inconsistent" and, conversely, that "consistency" might require identical requirements. The Committee believes that "complementary" is a formulation that helps communicate the importance of the Federal government having requirements that can meet the needs of different agencies and programs while fitting together in a coordinated manner to provide government-wide information security.

This subsection also provides for the submission of NIST-developed information security standards to OMB for promulgation; deadlines for the developing standards and guidelines; and mandates to avoid prescriptive technology-specific requirements, provide for flexibility to permit alternative solutions to information security problems, and ensure the use of performance-based standards to the greatest extent possible.

Subsection 303(c)(5) emphasizes that open, transparent standards activities undertaken by NIST, such as the development and publication of the Advanced Encryption Standard, promote flexibility by permitting alternative hardware and software solutions to provide equivalent levels of protection and enable vendors to offer a variety of solutions to meet customer needs. By contrast, when standards development has not been open and the resulting NIST standard is not published and flexibly implementable, the standard has failed to gain broad acceptance and use. The Clipper Chip is an example of this failed effort.

Subsection (d), strengthens NIST's organizational attention and commitment to information security by establishing a NIST Office for Information Security Programs.

Subsection (e) strengthens other current NIST responsibilities relating to standards development, technical assistance, research, and evaluation. First, NIST is to submit standards to OMB along with recommendations as to the extent to which they should be made mandatory. Second, NIST is to provide assistance to agencies with regard to compliance with standards and guidelines, detecting and handling security incidents, and information security policies and procedures. Third, NIST is to conduct research, as needed, into information security matters. Fourth, NIST is to develop and periodically revise information security performance indicators and measures. Fifth, NIST is to evaluate private sector information security policies and practices and assess their potential application in government. Sixth, NIST is to evaluate national security policies and practices and assess their potential application to other agencies. Seventh, NIST is to periodically assess the effectiveness of its standards and guidelines, and undertake revisions as appropriate. Eighth, NIST is to solicit and consider its advisory board's recommendations with regards to proposed NIST standards and guidelines. Ninth, NIST is to prepare an annual public report on its activities.

Finally, subsection (f) revises Computer Security definitions to conform to the definitions in 44 U.S.C. 3532, as amended by FISMA.

SEC. 304. INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

This section revises section 21 of the NIST Act (15 U.S.C. 278g–4) regarding the Computer System Security and Privacy Advisory Board. The subchapter strengthens the board and updates its name and mission to ensure that it has sufficient independence and resources to consider information security issues and provide useful advice to NIST.

At § 278g–4(a), FISMA changes the board's name from the Computer System Security and Privacy Advisory Board (CSSPAB) to the Information Security and Privacy Advisory Board, consistent with general use of the term "information security."

At § 278g–4(b)(2), FISMA strengthens the role of the board by mandating that it provide advice not only to NIST in developing standards, but also to OMB, which is to promulgate the NIST-developed standards.

At § 278g–4(b)(3), FISMA strengthens the role of the board by requiring that it prepare an annual report. For a number of years the CSSPAB produced annual reports that reflect the board's consideration of important security issues. In more recent years, the board did not produce such reports. The Committee believes Federal information security could be assisted by the preparation and dissemination of these reports.

At § 278g–4(f), FISMA strengthens the board by authorizing it to hold its meetings where and when it chooses. To function as an effective advisory board, it would be useful for the board to be able to hold meetings in locations easily accessible by expert witnesses and interested Federal employees as well as members of the public.

At § 278g–4(h), FISMA revises Computer Security Act definitions consistent with its other definitional changes.

SEC. 305. TECHNICAL AND CONFORMING AMENDMENTS

Sec. 305(a) repeals sections 5 and 6 of the Computer Security Act of 1987, at 40 U.S.C. 11332(b) and (c). These sections are superseded by the new legislation. Section 5 of the Computer Security Act covers computer system security training. These provisions are unnecessary given FISMA's training provisions at § 3534(a)(3)(D) & (4), (b)(4), and (d)(1)(B). Section 6 of the Computer Security Act requires the identification of systems containing sensitive information and the development of systems security plans. This section is unnecessary given the overall scheme and specific requirements for agency risk-based management of information and information systems supporting agency operations and assets. With regard to the other substantive provisions of the Computer Security Act, FISMA, at sec. 302, amends section 4 (section 5131 of the Clinger-Cohen Act, at 40 U.S.C. 11331), and, at sec. 303 and 304, amends section 3 (sections 20 & 21 of the NIST Act, 15 U.S.C. 278g–3 & 4).

Sec. 305(b) repeals sec. 1062 of Pub. L. 106–398, the section of the Government Information Security Reform (GISRA) provisions of the 2001 Defense Authorization Act, not directly superseded by FISMA, which is intended to represent a complete substitute revision of GISRA. FISMA, sec. 301(b)(1), supersedes GISRA, sec. 1061; FISMA, sec. 301(c)(1)(B), supersedes GISRA, sec. 1063; FISMA, sec. 301(c)(2), supersedes GISRA, sec. 1062(g); FISMA, sec. 301(b)(2), supersedes GISRA, sec. 1064; and FISMA, sec. 402, supersedes GISRA, sec. 1065. Accordingly, FISMA, sec. 305(b), repeals the remaining provisions in GISRA, sec. 1062.

The establishment of specific information security requirements for OMB and Federal agencies by FISMA obviates the need for several provisions in the Paperwork Reduction Act (PRA), which describe general information security mandates. Accordingly, FISMA, at sec. 305(c), amends the PRA to strike duplicative language and otherwise update references to refer to FISMA. Further, at sec. 305(c)(2), FISMA amends the PRA to establish a requirement for a regular inventory of major information systems to support information security and broader information resources management decision-making.

SEC. 306. CONSTRUCTION

This section provides that nothing in the subchapter affects the authority of NIST or the Department of Commerce concerning the development and promulgation of information standards or guidelines under paragraphs (1) and (2) of section 20(a) of the NIST Act. This is to ensure that the transfer of authority to promulgate information security standards from Commerce to OMB not affect or otherwise interfere with the continuing responsibility of NIST and Commerce with regard to other information system standards.

TITLE IV—AUTHORIZATION OF APPROPRIATIONS AND EFFECTIVE DATES

SEC. 401. AUTHORIZATION OF APPROPRIATIONS

The section authorizes such sums as are necessary to carry out titles I and II for fiscal years 2003 through 2007, except where authorization is specifically provided in those titles.

SEC. 402. EFFECTIVE DATES

The section provides that titles I and II and their amendments are to be effective 120 days after enactment, except sections 207, 216, and 217, which are to be effective on the date of enactment. The section further provides that title III and IV shall take effect on the date of enactment.

TITLE V—CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY

SEC. 501. SHORT TITLE

The section provides that this title may be cited as the "Confidential Information Protection and Statistical Efficiency Act of 2002."

SEC. 502. DEFINITIONS

This section contains definitions of nine terms including; "agent," "identifiable form," "business data," "statistical activities," "statistical purpose, and nonstatistical purpose".

SEC. 503. COORDINATION AND OVERSIGHT OF POLICIES

The section specifies that the Director of OMB shall coordinate and oversee the confidentiality and information sharing policies and rules established by the various agencies under this title. Among other required reports, each designated statistical agency is required to report to the Director of OMB and to the House Committee on Government Reform and the Senate Committee on Governmental Affairs on actions taken under subtitle B of this title.

SEC. 504. EFFECT ON OTHER LAWS

The section provides that this title does not affect other laws, including Bureau of Census provisions providing for limited disclosures of business statistical information. Also specifies that State laws on the confidentiality of data are not preempted and that statistical information may be disclosed to a law enforcement agency for prosecutions for the submission of false statistical information.

Subtitle A—Confidential Information Protection

SEC. 511. FINDINGS AND PURPOSES

The section lists five findings including: that protecting the confidentiality interests of individuals or organizations who provide information for federal statistical programs serves both the interests of the public and the needs of society and that ensuring that information provided for statistical purposes receives protection is essential in continuing public cooperation in statistical programs. The section further lists the proposes for the title which include ensuring that information supplied to an agency for statistical purposes under a pledge of confidentiality is used only for statistical purposes and to safeguarding individually identifiable information acquired under a confidentiality pledge by controlling access to and uses made of such information.

SEC. 512. LIMITATIONS ON USE AND DISCLOSURE OF DATA AND INFORMATION

The section would protect information submitted to all agencies under a pledge of confidentiality and for statistical purposes and sets strict rules for the confidentiality of the data provided. It prohibits disclosure of the data or information in an identifiable form for any use other than a statistical one except with the informed consent of the person or organization providing the information. Such disclosure is only authorized when approved by an agency head and it is not otherwise prohibited by law.

SEC. 513. FINES AND PENALTIES

The section provides felony criminal penalties (up to 5 years in jail and a maximum $250,000 fine) for any knowing and willful disclosures by an agency officer, employee, or agent of information acquired exclusively for statistical purposes in violation of this title.

Subtitle B—Statistical Efficiency

SEC. 521. FINDINGS AND PURPOSES

The section lists six findings including: that federal statistics are an important source of information for public and private decision makers, the quality of federal statistics depends on the willingness of businesses to respond to surveys, and enhanced sharing of business data among the Bureau of the Census, the Bureau of Economic Analysis, and the Bureau of Labor Statistics for exclusively statistical purposes will improve their ability to track more accurately the changing nature of U.S. business. The section further provides that the purposes of this subtitle include authorizing the sharing of business data among the Bureaus of Census, Economic Analysis, and Labor Statistics for only statistical purposes, to reduce paperwork burdens on businesses that provide information to the Government, and to improve the comparability and accuracy of Federal economic statistics

SEC. 522. DESIGNATION OF STATISTICAL AGENCIES

This section designates that the U.S. Census Bureau, the U.S. Bureau of Labor Statistics and the U.S. Bureau of Economic Analysis as statistical agencies for the purposes of this subtitle.

SEC. 523. RESPONSIBILITIES OF DESIGNATED STATISTICAL AGENCIES

The section provides that the head of each of the three statistical agencies is to identify opportunities to eliminate duplication in the collection and reporting of statistical business data, enter into joint projects to improve the quality and reduce costs, protect the confidentiality of individually identifiable information by, among other things, emphasizing to employees and agents the importance of protecting the confidentiality of identifiable information, and implementing appropriate measures to assure security.

SEC. 524. SHARING OF BUSINESS DATA AMONG DESIGNATED STATISTICAL AGENCIES

This section would allow that the U.S. Census Bureau, the U.S. Bureau of Labor Statistics and the U.S. Bureau of Economic Analysis to enter into a written agreement to provide business data in an identifiable form in their possession to each other and specifies that any information sharing will be accorded all of the confidentiality provisions of subtitle A and other existing laws. The written agreement must specify: (1) the business data to be shared; (2) the statistical purpose for which it can be used; (3) who in each agency can examine the data; and (4) appropriate security procedures to safeguard the confidentiality of the business data.

SEC. 525. LIMITATIONS ON USE OF BUSINESS DATA PROVIDED BY STATISTICAL AGENCIES

The section provides that any shared business data under this subtitle shall be used exclusively for statistical purposes and that any publication of business data shall occur only in a form where the data is not personally identifiable.

SEC. 526. CONFORMING AMENDMENTS

The section provides for amendments to current law, including adding a new section 402 to chapter 10 of title 13 of the U.S. Code allowing the Census Bureau to provide business data to the Bureaus of Economic Analysis and Labor Statistics.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, November 14, 2002.

Hon. DAN BURTON,
Chairman, Committee on Government Reform,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 2458, the E-Government Act of 2002.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Matthew Pickford.

Sincerely,

DAN L. CRIPPEN,
Director.

Enclosure.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

H.R. 2458—E-Government Act of 2002

Summary: H.R. 2458 would authorize appropriations for programs to improve the coordination and deployment of information technology, as well as improve electronic access to government information and services. The bill would:

- Establish an Office of Electronic Government within the Office of Management and Budget (OMB),
- Create a Chief Information Officers Council,
- Establish an E-Government Fund administered through the General Services Administration (GSA),
- Create an exchange program between the federal government and the private sector to promote information technology management,
- Expand the use of information technology share-in-savings (SIS) pilot programs through 2009, and
- Allow the Census Bureau, the Bureau of Economic Analysis (BEA), and the Bureau of Labor Statistics (BLS) to share business data subject to certain confidentiality restrictions and would create new criminal penalties for violations of these restrictions.

Assuming appropriation of the necessary amounts, we estimate that implementing H.R. 2458 would cost about $60 million in 2003 and about $600 million over the 2003–2007 period. That spending could be partially offset by savings of up to $10 million a year after a two- or three-year implementation period, assuming that appropriations for the Census Bureau and BLS are reduced accordingly. We also estimate that enacting the bill would increase direct spending by $7 million over the 2003–2007 period and $22 million over the 2003–2012 period. That spending would be for the estimated cost of unfunded termination liability of SIS contracts authorized by the bill. CBO estimates that the provisions regarding civil and criminal penalties would have no significant effect on revenues.

H.R. 2458 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments. Provisions of title II would benefit the District of Columbia by authorizing employees of the Office of the Chief Technology Officer to be assigned to a private-sector organization or an employee of such organization to be assigned to the office. Other provisions of title II could benefit state and local governments by authorizing the General Services Administration to allow them access to certain federal purchasing schedules.

Estimated cost to the Federal Government: As shown in the following table, CBO estimates that implementing H.R. 2458 would cost about $570 million over the 2003–2007 period, subject to ap-

propriation of the necessary amounts, as well as $8 million in new direct spending over the same period. The costs of this legislation fall within budget functions 370 (commerce and housing credit), 500 (education, training, employment, and social services), and 800 (general government).

	By fiscal year, in millions of dollars—				
	2003	2004	2005	2006	2007
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Specified Authorization Level	100	74	122	170	20
Estimated Outlays	59	57	76	112	20
Electronic Government Programs:					
Estimated Authorization Level	3	31	34	36	191
Estimated Outlays	2	32	34	36	165
BLS and Census Savings:					
Estimated Authorization Level	0	0	−10	−10	−10
Estimated Outlays	0	0	−10	−10	−10
Total Estimated Authorization Level	103	105	146	196	201
Total Estimated Outlays	61	89	100	138	175
CHANGES IN DIRECT SPENDING					
Estimated Budget Authority	(1)	1	1	2	3
Estimated Outlays	(1)	1	1	2	3

[1] =Less than $500,000.

Basis of estimate: For this estimate, we assume that the necessary amounts will be provided each year and that spending will follow historical patterns for similar activities. CBO estimates that H.R. 2458 would authorize the appropriation of approximately $750 million over the 2003–2007 period for managing and promoting electronic government services and processes. This estimate assumes that funding would be adjusted for anticipated inflation.

Specific authorizations

The bill would authorize the appropriation of $486 million over the 2003–2007 period for the following activities:

- $369 million for the GSA to operate the E-Government Fund for interagency projects, develop electronic signatures for executive agencies, maintain and promote the federal Internet portal, and to study disparities in access to the internet;
- $100 million for the National Institute of Standards and Technology to create a new Office for Information Security Programs, which would conduct research and issue standards related to the security of federal information systems; and
- $17 million for ongoing efforts, including developing and maintaining databases and websites for federally funded research, information technology training, and education.

Estimated authorizations

The authorizations specified in H.R. 2458 would cover different time periods. For example, some are only for fiscal year 2003, but others extend for four or five years. In addition to these specified authorizations, H.R. 2458 also would authorize such sums as necessary during the next five years to fund electronic government programs. These include operating the E-Government Fund; maintaining and promoting the federal Internet portal; developing electronic signatures; developing and maintaining databases and websites for federally funded research; and supporting information

technology training, research, reports, and education. CBO estimates that continuing the activities authorized by the bill would require the appropriation of $295 million over the 2003–2007 period, assuming adjustments for anticipated inflation.

Savings

The use of electronic information systems to collect information form the public and to provide government services could reduce administrative costs at federal agencies; however, CBO has no basis for estimating any such savings over the next few years.

CBO also expects that allowing the Census Bureau and BLS to share business data could generate cost savings for the two agencies. Under current law, statistical agencies cannot exchange such data, and therefore sometimes collect duplicative information. For example, the Census Bureau and BLS together typically spend about $150 million a year to collect and process data for their own independent lists of business establishments. Under H.R. 5215, these agencies could create one master list and potentially reduce total data collection and maintenance costs. Based on information from the two agencies, OMB and the General Accounting Office, CBO estimates that, after an implementation period of two or three years, the Census Bureau and BLS could achieve savings of up to $10 million annually, assuming that appropriations for the two agencies are reduced accordingly.

Direct spending and revenues

H.R. 2458 would authorize federal agencies to use SIS contracts for the purchase of information technology consultants and hardware through September 2009. The bill would allow up to five contracts per year in fiscal years 2003 through 2005 and up to 10 contracts per year in fiscal year 2006 through 2009.

A SIS contract can be used to procure products and services without an up-front payment. Payment for such goods and services would be made from any operational savings or increased collections generated from the contract. In addition, H.R. 2458 would allow agencies to enter into SIS contracts without funds available for the termination cost of the contract. The bill would limit the amount of such unfunded termination liability to $5 million per contract (or 25 percent of the termination costs, whichever is less).

For this estimate, we assume that the new authority provided by the bill will be fully used. Based on information from GSA about the current use of SIS contracts, CBO estimates that 10 percent of the SIS contracts authorized by H.R. 2458 would be terminated before completion. Assuming that SIS contracts have an average duration of five years and that the maximum termination liability could be incurred in any year, we estimate this provision would cost $7 million over the 2003–2007 period and $22 over the 2003–2012 period.

Intergovernmental and private-sector impact: H.R. 2458 contains no intergovernmental or private-sector mandates as defined in UMRA and would impose no costs on state, local, or tribal governments. Provisions of title II would benefit the District of Columbia by authorizing employees of the Office of the Chief Technology Officer to be assigned to a private-sector organization or an employee of such organization to be assigned to the office. Other provisions

of title II could benefit state and local governments by authorizing the General Services Administration to allow them access to certain federal purchasing schedules.

Previous CBO estimate: On June 7, 2002, CBO transmitted a cost estimate for S. 803, the E-Government Act of 2002, as ordered reported by the Senate Committee on Governmental Affairs on March 21, 2002. These pieces of legislation are very similar, however, the House bill would authorize the appropriation of about $100 million more than S. 803. In addition, the House bill would authorize SIS contracts, and S. 803 would not.

Title V of H.R. 2458, concerning sharing business data among federal statistical agencies, is identical to H.R. 5215, as ordered reported by the House Committee on Government Reform on October 9, 2002, for which CBO transmitted a cost estimate on November 8, 2002. The estimated budgetary effects of those provisions are the same.

Estimate prepared by: Census and BLS: Ken Johnson and Christina Hawley Sadoti; Other Federal Costs: Matthew Pickford; Impact on State, Local, and Tribal Governments: Susan Sieg Tompkins; and Impact on the Private Sector: Paige Piper/Bach.

Estimated approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

TITLE 44, UNITED STATES CODE

PUBLIC PRINTING AND DOCUMENTS

* * * * * * *

CHAPTER 35—COORDINATION OF FEDERAL INFORMATION POLICY

SUBCHAPTER I—FEDERAL INFORMATION POLICY

* * * * * * *

SUBCHAPTER II—INFORMATION SECURITY

SUBCHAPTER I—FEDERAL INFORMATION POLICY

* * * * * * *

§ 3504. Authority and functions of Director

(a) * * *

* * * * * * *

(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; *and*

(2) oversee and coordinate compliance with sections 552 and 552a of title 5, sections 20 and 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3 and 278g–4), **[**sections 11331 and 11332(b) and (c) of title 40**]** *section 11331 of title 40 and subchapter II of this chapter*, and related information management laws**[**; and**]**.

[(3) require Federal agencies, consistent with the the standards and guidelines promulgated under sections 11331 and 11332(b) and (c) of title 40, 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.**]**

* * * * * * *

§ 3505. Assignment of tasks and deadlines

(a) * * *

* * * * * * *

(c)(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.

§ 3506. Federal agency responsibilities

(a) * * *

* * * * * * *

(g) 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; *and*

(2) assume responsibility and accountability for compliance with and coordinated management of sections 552 and 552a of title 5, [section 11332 of title 40] *subchapter II of this chapter*, and related information management laws[; and].

[(3) consistent with section 11332 of title 40, 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.]

* * * * * * *

[SUBCHAPTER II—INFORMATION SECURITY

[§ 3531. Purposes

[The purposes of this subchapter are the following:

[(1) To provide a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support Federal operations and assets.

[(2)(A) To recognize the highly networked nature of the Federal computing environment including the need for Federal Government interoperability and, in the implementation of improved security management measures, assure that opportunities for interoperability are not adversely affected.

[(B) To 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) To provide for development and maintenance of minimum controls required to protect Federal information and information systems.

[(4) To provide a mechanism for improved oversight of Federal agency information security programs.

[§ 3532. Definitions

[(a) Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

[(b) In this subchapter:

[(1) The term "information technology" has the meaning given that term in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401).

[(2) The term "mission critical system" means any telecommunications or information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, that—

[(A) is defined as a national security system under section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452);

[(B) 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 classified in the interest of national defense or foreign policy; or

[(C) processes any information, the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.

[§ 3533. Authority and functions of the Director

[(a)(1) The Director shall establish governmentwide policies for the management of programs that—

[(A) support the cost-effective security of Federal information systems by promoting security as an integral component of each agency's business operations; and

[(B) include information technology architectures as defined under section 5125 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1425).

[(2) Policies under this subsection shall—

[(A) be founded on a continuing risk management cycle that recognizes the need to—

[(i) identify, assess, and understand risk; and

[(ii) determine security needs commensurate with the level of risk;

[(B) implement controls that adequately address the risk;

[(C) promote continuing awareness of information security risk; and

[(D) continually monitor and evaluate policy and control effectiveness of information security practices.

[(b) The authority under subsection (a) includes the authority to—

[(1) oversee and develop policies, principles, standards, and guidelines for the handling of Federal information and information resources to improve the efficiency and effectiveness of governmental operations, including principles, policies, and guidelines for the implementation of agency responsibilities under applicable law for ensuring the privacy, confidentiality, and security of Federal information;

[(2) consistent with the standards and guidelines promulgated under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) and sections 5 and 6 of the Computer Security

Act of 1987 (40 U.S.C. 1441 note; Public Law 100–235; 101 Stat. 1729), require Federal agencies 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;

[(3) direct the heads of agencies to—

[(A) identify, use, and share best security practices;

[(B) develop an agencywide information security plan;

[(C) incorporate information security principles and practices throughout the life cycles of the agency's information systems; and

[(D) ensure that the agency's information security plan is practiced throughout all life cycles of the agency's information systems;

[(4) oversee the development and implementation of standards and guidelines relating to security controls for Federal computer systems by the Secretary of Commerce through the National Institute of Standards and Technology under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) and section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3);

[(5) oversee and coordinate compliance with this section in a manner consistent with—

[(A) sections 552 and 552a of title 5;

[(B) sections 20 and 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3 and 278g–4);

[(C) section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

[(D) sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 1441 note; Public Law 100–235; 101 Stat. 1729); and

[(E) related information management laws; and

[(6) take any authorized action under section 5113(b)(5) of the Clinger-Cohen Act of 1996 (40 U.S.C. 1413(b)(5)) that the Director considers appropriate, including any action involving the budgetary process or appropriations management process, to enforce accountability of the head of an agency for information resources management, including the requirements of this subchapter, and for the investments made by the agency in information technology, including—

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

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

[(C) using other authorized administrative controls over appropriations to restrict the availability of funds for information resources.

[(c) The authorities of the Director under this section (other than the authority described in subsection (b)(6))—

[(1) shall be delegated to the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President in the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2);

[(2) shall be delegated to the Secretary of Defense in the case of systems described under subparagraph (C) of section 3532(b)(2) 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; and

[(3) in the case of all other Federal information systems, may be delegated only to the Deputy Director for Management of the Office of Management and Budget.

[§ 3534. Federal agency responsibilities

[(a) The head of each agency shall—

[(1) be responsible for—

[(A) adequately ensuring the integrity, confidentiality, authenticity, availability, and nonrepudiation of information and information systems supporting agency operations and assets;

[(B) developing and implementing information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the agency; and

[(C) ensuring that the agency's information security plan is practiced throughout the life cycle of each agency system;

[(2) ensure that appropriate senior agency officials are responsible for—

[(A) assessing the information security risks associated with the operations and assets for programs and systems over which such officials have control;

[(B) determining the levels of information security appropriate to protect such operations and assets; and

[(C) periodically testing and evaluating information security controls and techniques;

[(3) delegate to the agency Chief Information Officer established under section 3506, or a comparable official in an agency not covered by such section, the authority to administer all functions under this subchapter including—

[(A) designating a senior agency information security official who shall report to the Chief Information Officer or a comparable official;

[(B) developing and maintaining an agencywide information security program as required under subsection (b);

[(C) ensuring that the agency effectively implements and maintains information security policies, procedures, and control techniques;

[(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

[(E) assisting senior agency officials concerning 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 senior agency officials, periodically—

[(A)(i) evaluates the effectiveness of the agency information security program, including testing control techniques; and

[(ii) implements appropriate remedial actions based on that evaluation; and

[(B) reports to the agency head on—

[(i) the results of such tests and evaluations; and

[(ii) the progress of remedial actions.

[(b)(1) Each agency shall develop and implement an agencywide information security program to provide information security for the operations and assets of the agency, including operations and assets provided or managed by another agency.

[(2) Each program under this subsection shall include—

[(A) periodic risk assessments that consider internal and external threats to—

[(i) the integrity, confidentiality, and availability of systems; and

[(ii) data supporting critical operations and assets;

[(B) policies and procedures that—

[(i) are based on the risk assessments required under subparagraph (A) that cost-effectively reduce information security risks to an acceptable level; and

[(ii) ensure compliance with—

[(I) the requirements of this subchapter;

[(II) policies and procedures as may be prescribed by the Director; and

[(III) any other applicable requirements;

[(C) security awareness training to inform personnel of—

[(i) information security risks associated with the activities of personnel; and

[(ii) responsibilities of personnel in complying with agency policies and procedures designed to reduce such risks;

[(D) periodic management testing and evaluation of the effectiveness of information security policies and procedures;

[(E) a process for ensuring remedial action to address any significant deficiencies; and

[(F) procedures for detecting, reporting, and responding to security incidents, including—

[(i) mitigating risks associated with such incidents before substantial damage occurs;

[(ii) notifying and consulting with law enforcement officials and other offices and authorities;

[(iii) notifying and consulting with an office designated by the Administrator of General Services within the General Services Administration; and

[(iv) notifying and consulting with an office designated by the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the

President for incidents involving systems described under subparagraphs (A) and (B) of section 3532(b)(2).

[(3) Each program under this subsection is subject to the approval of the Director and is required to be reviewed at least annually by agency program officials in consultation with the Chief Information Officer. In the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2), the Director shall delegate approval authority under this paragraph to the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President.

[(c)(1) Each agency shall examine 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 I of this chapter;

[(C) performance and results based management under the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.);

[(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 through 2805 of title 39; and

[(E) financial management under—

[(i) chapter 9 of title 31, United States Code, 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);

[(ii) the Federal Financial Management Improvement Act of 1996 (31 U.S.C. 3512 note) (and the amendments made by that Act); and

[(iii) the internal controls conducted under section 3512 of title 31.

[(2) Any significant deficiency in a policy, procedure, or practice identified under paragraph (1) shall be reported as a material weakness in reporting required under the applicable provision of law under paragraph (1).

[(d)(1) In addition to the requirements of subsection (c), each agency, in consultation with the Chief Information Officer, 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, which are necessary to implement the program required under subsection (b)(1).

[(2) The description under paragraph (1) shall be based on the risk assessment required under subsection (b)(2)(A).

[§ 3535. Annual independent evaluation

[(a)(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency.

[(2) Each evaluation by an agency under this section shall include—

[(A) testing of the effectiveness of information security control techniques for an appropriate subset of the agency's information systems; and

[(B) an assessment (made on the basis of the results of the testing) of the compliance with—

[(i) the requirements of this subchapter; and

[(ii) related information security policies, procedures, standards, and guidelines.

[(3) The Inspector General or the independent evaluator performing an evaluation under this section may use an audit, evaluation, or report relating to programs or practices of the applicable agency.

[(b)(1)(A) Subject to subparagraph (B), for agencies with Inspectors General appointed under the Inspector General Act of 1978 (5 U.S.C. App.) or any other law, the annual evaluation required under this section or, in the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2), an audit of the annual evaluation required under this section, shall be performed by the Inspector General or by an independent evaluator, as determined by the Inspector General of the agency.

[(B) For systems described under subparagraphs (A) and (B) of section 3532(b)(2), the evaluation required under this section shall be performed only by an entity designated by the Secretary of Defense, the Director of Central Intelligence, or another agency head as designated by the President.

[(2) For any agency to which paragraph (1) does not apply, the head of the agency shall contract with an independent evaluator to perform the evaluation.

[(c) Each year, not later than the anniversary of the date of the enactment of this subchapter, the applicable agency head shall submit to the Director—

[(1) the results of each evaluation required under this section, other than an evaluation of a system described under subparagraph (A) or (B) of section 3532(b)(2); and

[(2) the results of each audit of an evaluation required under this section of a system described under subparagraph (A) or (B) of section 3532(b)(2).

[(d)(1) The Director shall submit to Congress each year a report summarizing the materials received from agencies pursuant to subsection (c) in that year.

[(2) Evaluations and audits of evaluations of systems under the authority and control of the Director of Central Intelligence and evaluations and audits of evaluation of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available only to the appropriate oversight committees of Congress, in accordance with applicable laws.

[(e) Agencies and evaluators shall take appropriate actions to ensure the protection of information, the disclosure of which may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws.

[§ 3536. Expiration

[This subchapter shall not be in effect after the date that is two years after the date on which this subchapter takes effect.]

SUBCHAPTER II—INFORMATION SECURITY

§ 3531. 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 government-wide 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.

§ 3532. 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 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; and

(C) availability, which means ensuring timely and reliable access to and use of information;

(2) 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—

(A) 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) is critical to the direct fulfillment of military or intelligence missions,

except that this subparagraph does not include a system that is used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or

(B) 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; and

(3) the term "information technology" has the meaning given that term in section 11101 of title 40.

§ 3533. Authority and functions of the Director

(a) 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 the promulgation of standards and guidelines 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 3534(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 3536; 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 3535;

(B) significant deficiencies in agency information security practices;

(C) planned remedial action to address such deficiencies; and

(D) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(e)(7) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3).

(b) 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.

§ 3534. Federal agency responsibilities

(a) 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 by the Director 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 3533 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) Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3533(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 evaluation under section 3535;

(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 3536(b), including—

(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 3536; 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) 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 of this chapter;

(C) information technology management under subtitle III of title 40;

(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, (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)(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) Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

§ 3535. Annual independent evaluation

(a)(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 by an agency 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) Subject to subsection (c)—

(1) for each agency with an Inspector General appointed under the Inspector General Act of 1978, 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) 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) 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)(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) 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)(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3533(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) 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.

§ 3536. Federal information security incident center

(a) 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 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) 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.

§ 3537. 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.

§ 3538. 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.

§ 3539. Effect on existing law

Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards 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, or the disclosure of information to the Congress or the Comptroller General of the United States.

CHAPTER 36—MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

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 the governing body of any Indian tribe, band, nation, or other organized group or community, including any Alaska Native village or regional or village corporation as defined in or established pursuant to the Alaska Native Claims Settlement Act (43 U.S.C. 1601 et seq.), which is recognized as eligible for the special programs and services provided by the United States to Indians because of their status as Indians.

§ 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 under section 11331 of title 40, to be developed by the National Institute of Standards and Technology and promulgated by the Secretary of Commerce, 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.

§ 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 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.

(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.

§ 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.

§ 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 sci-

entific 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.

§ 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, UNITED STATES CODE

* * * * * * *

SUBTITLE I—FEDERAL PROPERTY AND ADMINISTRATIVE SERVICES

* * * * * * *

CHAPTER 3—ORGANIZATION OF GENERAL SERVICES ADMINISTRATION

SUBCHAPTER I—GENERAL

Sec.
301. Establishment.

* * * * * * *

305. Electronic Government and information technologies.

* * * * * * *

SUBCHAPTER I—GENERAL

* * * * * * *

§ 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.

* * * * * * *

CHAPTER 5—PROPERTY MANAGEMENT

* * * * * * *

SUBCHAPTER I—PROCUREMENT AND WAREHOUSING

§ 502. Services for other entities

(a) * * *

* * * * * * *

(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 a tribal organization, as defined in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

(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)).

* * * * * * *

SUBTITLE III—INFORMATION TECHNOLOGY MANAGEMENT

* * * * * * *

CHAPTER 113—RESPONSIBILITY FOR ACQUISITIONS OF INFORMATION TECHNOLOGY

SUBCHAPTER III—OTHER RESPONSIBILITIES

[§ 11331. Responsibilities regarding efficiency, security, and privacy of federal computer systems

[(a) DEFINITIONS.—In this section, the terms "federal computer system" and "operator of a federal computer system" have the meanings given those terms in section 20(d) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(d)).

[(b) STANDARDS AND GUIDELINES.—

[(1) AUTHORITY TO PRESCRIBE AND DISAPPROVE OR MODIFY.—

[(A) AUTHORITY TO PRESCRIBE.—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 Act (15 U.S.C. 278g–3(a)(2), (3)), the Secretary of Commerce shall prescribe standards and guidelines pertaining to federal computer systems. The Secretary shall make those standards compulsory and binding to the extent the Secretary determines necessary to improve the efficiency of operation or security and privacy of federal computer systems.

[(B) AUTHORITY TO DISAPPROVE OR MODIFY.—The President may disapprove or modify those standards and guidelines if the President determines that action to be in the public interest. The President's authority to disapprove or modify those standards and guidelines may not be delegated. Notice of disapproval or modification shall be published promptly in the Federal Register. On receiving notice of disapproval or modification, the Secretary shall immediately rescind or modify those standards or guidelines as directed by the President.

[(2) 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.

[(c) APPLICATION OF MORE STRINGENT STANDARDS.—The head of a federal agency may employ standards for the cost-effective security and privacy of sensitive information in a federal computer system in 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 contain at least the applicable standards the Secretary makes compulsory and binding.

[(d) WAIVER OF STANDARDS.—

[(1) AUTHORITY OF THE SECRETARY.—The Secretary may waive in writing compulsory and binding standards under subsection (b) if the Secretary determines that compliance would—

[(A) adversely affect the accomplishment of the mission of an operator of a federal computer system; or

[(B) cause a major adverse financial impact on the operator that is not offset by Federal Government-wide savings.

[(2) DELEGATION OF WAIVER AUTHORITY.—The Secretary may delegate to the head of one or more federal agencies authority to waive those standards to the extent the Secretary determines that action to be necessary and desirable to allow for timely and effective implementation of federal computer system standards. The head of the agency may redelegate that authority only to a chief information officer designated pursuant to section 3506 of title 44.

[(3) NOTICE.—Notice of each waiver and delegation shall be transmitted promptly to Congress and published promptly in the Federal Register.]

§ 11331. Responsibilities for federal information systems standards

(a) INFORMATION SECURITY STANDARDS.—

(1) IN GENERAL.—(A) 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 paragraph (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3(a)), promulgate information security standards pertaining to Federal information systems.

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

(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems under this subsection shall be developed, promulgated, enforced, and overseen as otherwise authorized by law and as directed by the President.

(3) AGENCY HEAD AUTHORITY.—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 subsection, if such standards—

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

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

(4) DECISIONS ON PROMULGATION OF STANDARDS.—(A) The decision regarding the promulgation of any standard by the Director under paragraphs (1) and (2) 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).

(B) 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.

(b) ADDITIONAL STANDARDS RELATING TO FEDERAL INFORMATION SYSTEMS.—

(1) IN GENERAL.—Except as provided under paragraph (2), the Secretary of Commerce shall, on the basis of proposed standards developed by the National Institute of Standards and Technology pursuant to paragraph (2) 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 Director of the Office of Management and Budget, promulgate standards pertaining to Federal information systems. The Secretary shall make such standards compulsory and binding to the extent that the Secretary determines necessary to improve the efficiency and effectiveness of the operation of Federal information systems.

(2) NATIONAL SECURITY SYSTEMS.—Standards and guidelines for national security systems under this subsection shall be developed, promulgated, enforced, and overseen as otherwise authorized by law and as directed by the President.

(3) AUTHORITY OF SECRETARY.—The authority conferred upon the Secretary of Commerce by this subsection shall be exercised subject to direction by the President and in coordination with the Director of the Office of Management and Budget to ensure fiscal and policy consistency.

(4) AGENCY HEAD AUTHORITY.—The head of an agency may employ standards for information systems that are more stringent than the standards promulgated by the Secretary of Commerce under this subsection, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

(c) DEFINITIONS.—In this section:

(1) FEDERAL INFORMATION SYSTEM.—The term "Federal information system" means an information system used or operated by an agency, by a contractor of an agency, or by another organization on behalf of an agency.

(2) INFORMATION SECURITY.—The term "information security" has the meaning given that term in section 3532(b)(1) of title 44.

(3) NATIONAL SECURITY SYSTEM.—The term "national security system" has the meaning given that term in section 3532(b)(2) of title 44.

§ 11332. Federal computer system security training and plan

(a) * * *

[(b) TRAINING—

[(1) IN GENERAL.—Each federal agency shall provide for mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each federal computer system within or under the supervision of the agency. The training shall be–

[(A) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the Act (15 U.S.C. 278g–3(a)(5)) and the regulations prescribed under paragraph (3) for federal civilian employees; or

[(B) provided by an alternative training program that the head of the agency approves after determining that the alternative training program is at least as effective in accomplishing the objectives of the guidelines and regulations.

[(2) TRAINING OBJECTIVES.—Training under this subsection shall be designed—

[(A) to enhance employees' awareness of the threats to, and vulnerability of, computer systems; and

[(B) to encourage the use of improved computer security practices.

[(3) REGULATIONS.—The Director of the Office of Personnel Management shall maintain regulations that establish the procedures and scope of the training to be provided federal civilian employees under this subsection and the manner in which the training is to be carried out.

[(c) PLAN.—

[(1) IN GENERAL.—Consistent with standards, guidelines, policies, and regulations prescribed pursuant to section 11331 of this title, each federal agency shall maintain a plan for the security and privacy of each federal computer system the agency identifies as being within or under its supervision and as containing sensitive information. The plan must be commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information contained in the system.

[(2) REVISION AND REVIEW.—The plan shall be revised annually as necessary and is subject to disapproval by the Director of the Office of Management and Budget.]

* * * * * * *

TITLE 31, UNITED STATES CODE

* * * * * * *

SUBTITLE I—GENERAL

* * * * * * *

CHAPTER 5—OFFICE OF MANAGEMENT AND BUDGET

SUBCHAPTER I—ORGANIZATION

SUBCHAPTER I—ORGANIZATION

* * * * * * *

§ 503. Functions of Deputy Director for Management

(a) * * *

(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:

(1) * * *

* * * * * * *

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

[(5)**]** *(6)* Provide leadership in management innovation, through—

(A) * * *

* * * * * * *

[(6)**]** *(7)* Work with State and local governments to improve and strengthen intergovernmental relations, and provide assistance to such governments with respect to intergovernmental programs and cooperative arrangements.

[(7)**]** *(8)* Review and, where appropriate, recommend to the Director changes to the budget and legislative proposals of agencies to ensure that they respond to program evaluations by, and are in accordance with general management plans of, the Office of Management and Budget.

[(8)**]** *(9)* Provide advice to agencies on the qualification, recruitment, performance, and retention of managerial personnel.

[(9)**]** *(10)* Perform any other functions prescribed by the Director.

* * * * * * *

§ 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 5, UNITED STATES CODE

* * * * * * *

PART III—EMPLOYEES

Subpart A—General Provisions

Subpart B—Employment and Retention

CHAPTER 31—AUTHORITY FOR EMPLOYMENT

* * * * * * *

SUBCHAPTER I—EMPLOYMENT AUTHORITIES

* * * * * * *

§ 3111. Acceptance of volunteer service

(a) * * *

* * * * * * *

(d) Notwithstanding section 1342 of title 31, the head of an agency may accept voluntary service for the United States under chapter 37 of this title and regulations of the Office of Personnel Management.

* * * * * * *

CHAPTER 37—INFORMATION TECHNOLOGY EXCHANGE PROGRAM

§ 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.

§ 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.

§ 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.

Subpart C—Employee Performance

CHAPTER 41—TRAINING

* * * * * * *

§ 4108. Employee agreements; service after training

(a) * * *

* * * * * * *

[(d) For purposes of this section, "training" includes a private sector assignment of an employee participating in the Executive Exchange Program of the President's Commission on Executive Exchange.**]**

* * * * * * *

Subpart F—Labor-Management and Employee Relations

* * * * * * *

CHAPTER 73—SUITABILITY, SECURITY, AND CONDUCT

* * * * * * *

SUBCHAPTER V—MISCONDUCT

* * * * * * *

§ 7353. Gifts to Federal employees

(a) * * *
(b)(1) * * *

* * * * * * *

(4) Nothing in this section precludes an employee of a private sector organization, while assigned to an agency under chapter 37, from continuing to receive pay and benefits from such organization in accordance with such chapter.

* * * * * * *

SECTION 303 OF THE JUDICIARY APPROPRIATIONS ACT, 1992

SEC. 303. (a) The Judicial Conference [shall hereafter] *may, only to the extent necessary,* prescribe reasonable fees, pursuant to sections 1913, 1914, 1926, 1930, and 1932 of title 28, United States Code, for collection by the courts under those sections for access to information available through automatic data processing equipment. These fees may distinguish between classes of persons, and shall provide for exempting persons or classes of persons from the fees, in order to avoid unreasonable burdens and to promote public access to such information. The Director of the Administrative Office of the United States Courts, under the direction of the Judicial Conference of the United States, shall prescribe a schedule of reasonable fees for electronic access to information which the Director is required to maintain and make available to the public.

* * * * * * *

TITLE 18, UNITED STATES CODE

* * * * * * *

PART I—CRIMES

* * * * * * *

CHAPTER 11—BRIBERY, GRAFT, AND CONFLICTS OF INTEREST

* * * * * * *

§ 207. Restrictions on former officers, employees, and elected officials of the executive and legislative branches

(a) * * *

* * * * * * *

(c) ONE-YEAR RESTRICTIONS ON CERTAIN SENIOR PERSONNEL OF THE EXECUTIVE BRANCH AND INDEPENDENT AGENCIES.—

(1) * * *

(2) PERSONS TO WHOM RESTRICTIONS APPLY.—(A) Paragraph (1) shall apply to a person (other than a person subject to the restrictions of subsection (d))—

(i) * * *

* * * * * * *

(iii) appointed by the President to a position under section 105(a)(2)(B) of title 3 or by the Vice President to a position under section 106(a)(1)(B) of title 3, **[**or**]**

(iv) employed in a position which is held by an active duty commissioned officer of the uniformed services who is serving in a grade or rank for which the pay grade (as specified in section 201 of title 37) is pay grade O–7 or above**[**.**]***; or*

(v) assigned from a private sector organization to an agency under chapter 37 of title 5.

* * * * * * *

(l) CONTRACT ADVICE BY FORMER DETAILS.—Whoever, being an employee of a private sector organization assigned to an agency under chapter 37 of title 5, within one year after the end of that assignment, knowingly represents or aids, counsels, or assists in representing any other person (except the United States) in connection with any contract with that agency shall be punished as provided in section 216 of this title.

* * * * * * *

§ 209. Salary of Government officials and employees payable only by United States

(a) * * *

* * * * * * *

(g)(1) This section does not prohibit an employee of a private sector organization, while assigned to an agency under chapter 37 of title 5, from continuing to receive pay and benefits from such organization in accordance with such chapter.

(2) For purposes of this subsection, the term "agency" means an agency (as defined by section 3701 of title 5) and the Office of the Chief Technology Officer of the District of Columbia.

* * * * * * *

CHAPTER 93—PUBLIC OFFICERS AND EMPLOYEES

* * * * * * *

§ 1905. Disclosure of confidential information generally

Whoever, being an officer or employee of the United States or of any department or agency thereof, any person acting on behalf of the Office of Federal Housing Enterprise Oversight, or agent of the Department of Justice as defined in the Antitrust Civil Process Act (15 U.S.C. 1311–1314), *or being an employee of a private sector organization who is or was assigned to an agency under chapter 37 of title 5,* publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets, processes, operations, style of work, or

apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law; shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.

* * * * * * *

SECTION 27 OF THE OFFICE OF FEDERAL PROCUREMENT POLICY ACT

SEC. 27. RESTRICTIONS ON DISCLOSING AND OBTAINING CONTRACTOR BID OR PROPOSAL INFORMATION OR SOURCE SELECTION INFORMATION.

(a) PROHIBITION ON DISCLOSING PROCUREMENT INFORMATION.—(1) A person described in paragraph (2) shall not, other than as provided by law, knowingly disclose contractor bid or proposal information or source selection information before the award of a Federal agency procurement contract to which the information relates. *In the case of an employee of a private sector organization assigned to an agency under chapter 37 of title 5, United States Code, in addition to the restriction in the preceding sentence, such employee shall not, other than as provided by law, knowingly disclose contractor bid or proposal information or source selection information during the three-year period after the end of the assignment of such employee.*

* * * * * * *

THE ACT OF JANUARY 8, 1988

(Public Law 100–238)

AN ACT making technical corrections relating to the Federal Employees' Retirement System, and for other purposes.

SEC. 125. ELIGIBILITY OF CERTAIN INDIVIDUALS TO PARTICIPATE IN THE THRIFT SAVINGS PLAN.

(a) * * *

* * * * * * *

(c) APPLICABILITY.—This section applies with respect to—

(1) any individual participating in the Civil Service Retirement System or the Federal Employees' Retirement System as—

(A) * * *

(B) an individual assigned from a Federal agency to a State or local government under subchapter VI of chapter 33 of title 5, United States Code; **[**or**]**

(C) an individual appointed or otherwise assigned to one of the cooperative extension services, as defined by section 1404(5) of the National Agricultural Research, Extension,

and Teaching Policy Act of 1977 (7 U.S.C. 3103(5)); [and] *or*

(D) an individual assigned from a Federal agency to a private sector organization under chapter 37 of title 5, United States Code; and

* * * * * * *

TITLE 10, UNITED STATES CODE

* * * * * * *

Subtitle A—General Military Law

* * * * * * *

PART IV—SERVICE, SUPPLY, AND PROCUREMENT

* * * * * * *

CHAPTER 131—PLANNING AND COORDINATION

* * * * * * *

§ 2224. Defense Information Assurance Program

(a) * * *

[(b) OBJECTIVES AND MINIMUM REQUIREMENTS.—(1)] *(b) OBJECTIVES OF THE PROGRAM.*—The objectives of the program shall be to provide continuously for the availability, integrity, authentication, confidentiality, nonrepudiation, and rapid restitution of information and information systems that are essential elements of the Defense Information Infrastructure.

[(2) The program shall at a minimum meet the requirements of sections 3534 and 3535 of title 44.]

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

(1) * * *

* * * * * * *

CHAPTER 137—PROCUREMENT GENERALLY

Sec.
2302. Definitions.

* * * * * * *

2332. Share-in-savings contracts.

* * * * * * *

§ 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 con-

tract 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. 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—

(i) may not exceed 5, in each of fiscal years 2003, 2004, and 2005; and

(ii) may not exceed 10, in each of fiscal years 2006, 2007, 2008, and 2009.

(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.

(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, 2009.

* * * * * * *

FEDERAL PROPERTY AND ADMINISTRATIVE SERVICES ACT OF 1949

* * * * * * *

TITLE III—PROCUREMENT PROCEDURE

* * * * * * *

SEC. 317. 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, United States Code) 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. 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 chapter applies in a fiscal year—

(i) may not exceed 5, in each of fiscal years 2003, 2004, and 2005; and

(ii) may not exceed 10, in each of fiscal years 2006, 2007, 2008, and 2009.

(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.

(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, 2009.

* * * * * * *

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

* * * * * * *

SEC. 20. [(a) The Institute shall—

(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

[(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(9) of title 44, United States Code;

[(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

[(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(9) of title 44, United States Code; and

[(B) those systems which are 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,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

[(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

[(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

[(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

[(b) In fulfilling subsection (a) of this section, the Institute is authorized—

[(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

[(2) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

[(3) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

[(4) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost-effective security and privacy of sensitive information in Federal computer systems; and

[(5) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

[(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

[(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

[(c) For the purposes of—

[(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3), and

[(2) performing research and conducting studies under subsection (b)(5),

the Institute shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the Institute determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

[(d) As used in this section—

[(1) the term "computer system"—

[(A) means 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

[(B) includes—
[(i) computers;
[(ii) ancillary equipment;
[(iii) software, firmware, and similar procedures;
[(iv) services, including support services; and
[(v) related resources;

[(2) the term "Federal computer system" means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function;

[(3) the term "operator of a Federal computer system" means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function;

[(4) the term "sensitive information" means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not 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; and

[(5) the term "Federal agency" has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.]

(a) 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, United States Code); and

(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.

(b) The standards and guidelines required by subsection (a) 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 na-

tional security system consistent with applicable requirements for national security systems, issued in accordance with law and as directed by the President.

(c) In developing standards and guidelines required by subsections (a) and (b), the Institute shall—

(1) consult with other agencies and offices and the private sector (including 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, United States Code—

(A) standards, as required under subsection (b)(1)(A), no later than 12 months after the date of the enactment of this section; and

(B) minimum information security requirements for each category, as required under subsection (b)(1)(C), no later than 36 months after the date of the enactment of this section;

(4) issue guidelines as required under subsection (b)(1)(B), no later than 18 months after the date of the enactment of this section;

(5) ensure that such standards and guidelines do not specify the use or procurement of certain products, including any specific hardware or software;

(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)(1) There is established in the Institute an Office for Information Security Programs.

(2) The Office for Information Security Programs shall be headed by a Director, who shall be a senior executive and shall be compensated at a level in the Senior Executive Service under section 5382 of title 5, United States Code, as determined by the Secretary of Commerce.

(3) The Director of the Institute shall delegate to the Director of the Office of Information Security Programs the authority to administer all functions under this section, except that any such delegation shall not relieve the Director of the Institute of responsibility for the administration of such functions. The Director of the Office of

Information Security Programs shall serve as principal adviser to the Director of the Institute on all functions under this section.

(e) The Institute shall—

(1) submit standards developed pursuant to subsection (a), 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, United States Code;

(2) provide assistance to agencies regarding—

(A) compliance with the standards and guidelines developed under subsection (a);

(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 21, regarding standards and guidelines developed under subsection (a) 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.

(f) As used in this section—

(1) the term "agency" has the same meaning as provided in section 3502(1) of title 44, United States Code;

(2) the term "information security" has the same meaning as provided in section 3532(b)(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, United States Code; and

(5) the term "national security system" has the same meaning as provided in section 3532(b)(2) of title 44, United States Code.

(g) There are authorized to be appropriated to the Secretary of Commerce $20,000,000 for each of fiscal years 2003, 2004, 2005,

2006, and 2007 to enable the National Institute of Standards and Technology to carry out the provisions of this section.

SEC. 21. (a) There is hereby established a [Computer System Security and Privacy Advisory Board] *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 [computer or telecommunications] *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 [computer or telecommunications technology] *information technology*, or related disciplines, but who are not employed by or representative of a producer of [computer or telecommunications equipment] *information technology*; and

(3) four members from the Federal Government who have [computer systems] *information system* management experience, including experience in [computer systems security] *information security* and privacy, at least one of whom shall be from the National Security Agency.

(b) The duties of the Board shall be—

(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to [computer systems security] *information security* and privacy;

[(2) to advise the Institute and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and]

(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 through review of proposed standards and guidelines developed under section 20; 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.

* * * * * * *

(f) The Board shall hold meetings at such locations and at such time and place as determined by a majority of the Board.

[(f)] *(g)* 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.

[(g) As used in this section, the terms "computer system" and "Federal computer system" have the meanings given in section 20(d) of this Act.]

(h) As used in this section, the terms "information system" and "information technology" have the meanings given in section 20.

* * * * * * *

SECTION 1062 OF THE FLOYD D. SPENCE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2001

[SEC. 1062. RESPONSIBILITIES OF CERTAIN AGENCIES.

[(a) DEPARTMENT OF COMMERCE.—Notwithstanding section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and except as provided under subsection (b), the Secretary of Commerce, through the National Institute of Standards and Technology and with technical assistance from the National Security Agency, as required or when requested, shall—

[(1) develop, issue, review, and update standards and guidance for the security of Federal information systems, including development of methods and techniques for security systems and validation programs;

[(2) develop, issue, review, and update guidelines for training in computer security awareness and accepted computer security practices, with assistance from the Office of Personnel Management;

[(3) provide agencies with guidance for security planning to assist in the development of applications and system security plans for such agencies;

[(4) provide guidance and assistance to agencies concerning cost-effective controls when interconnecting with other systems; and

[(5) evaluate information technologies to assess security vulnerabilities and alert Federal agencies of such vulnerabilities as soon as those vulnerabilities are known.

[(b) DEPARTMENT OF DEFENSE AND THE INTELLIGENCE COMMUNITY.—

[(1) IN GENERAL.—Notwithstanding any other provision of this subtitle (including any amendment made by this subtitle)—

[(A) the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President, shall, consistent with their respective authorities—

[(i) develop and issue information security policies, standards, and guidelines for systems described under subparagraphs (A) and (B) of section 3532(b)(2) of title 44, United States Code (as added by section 1061 of this Act), that provide more stringent protection, to the maximum extent practicable, than the policies, principles, standards, and guidelines required under section 3533 of such title (as added by such section 1061); and

[(ii) ensure the implementation of the information security policies, principles, standards, and guidelines described under clause (i); and

[(B) the Secretary of Defense shall, consistent with his authority—

[(i) develop and issue information security policies, standards, and guidelines for systems described under subparagraph (C) of section 3532(b)(2) of title 44, United States Code (as added by section 1061 of this Act), 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 provide more stringent protection, to the maximum extent practicable, than the policies, principles, standards, and guidelines required under section 3533 of such title (as added by such section 1061); and

[(ii) ensure the implementation of the information security policies, principles, standards, and guidelines described under clause (i).

[(2) MEASURES ADDRESSED.—The policies, principles, standards, and guidelines developed by the Secretary of Defense and the Director of Central Intelligence under paragraph (1) shall address the full range of information assurance measures needed to protect and defend Federal information and information systems by ensuring their integrity, confidentiality, authenticity, availability, and nonrepudiation.

[(c) DEPARTMENT OF JUSTICE.—The Attorney General shall review and update guidance to agencies on—

[(1) legal remedies regarding security incidents and ways to report to and work with law enforcement agencies concerning such incidents; and

[(2) lawful uses of security techniques and technologies.

[(d) GENERAL SERVICES ADMINISTRATION.—The Administrator of General Services shall—

[(1) review and update General Services Administration guidance to agencies on addressing security considerations when acquiring information technology; and

[(2) assist agencies in—

[(A) fulfilling agency responsibilities under section 3534(b)(2)(F) of title 44, United States Code (as added by section 1061 of this Act); and

[(B) the acquisition of cost-effective security products, services, and incident response capabilities.

[(e) OFFICE OF PERSONNEL MANAGEMENT.—The Director of the Office of Personnel Management shall—

[(1) review and update Office of Personnel Management regulations concerning computer security training for Federal civilian employees;

[(2) assist the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and computer security best practices; and

[(3) work with the National Science Foundation and other agencies on personnel and training initiatives (including scholarships and fellowships, as authorized by law) as necessary to ensure that the Federal Government—

[(A) has adequate sources of continuing information security education and training available for employees; and

[(B) has an adequate supply of qualified information security professionals to meet agency needs.

[(f) INFORMATION SECURITY POLICIES, PRINCIPLES, STANDARDS, AND GUIDELINES.—

[(1) ADOPTION OF POLICIES, PRINCIPLES, STANDARDS, AND GUIDELINES OF OTHER AGENCIES.—The policies, principles, standards, and guidelines developed under subsection (b) by the Secretary of Defense, the Director of Central Intelligence,

and another agency head as designated by the President may be adopted, to the extent that such policies are consistent with policies and guidance developed by the Director of the Office of Management and Budget and the Secretary of Commerce—

[(A) by the Director of the Office of Management and Budget, as appropriate, for application to the mission critical systems of all agencies; or

[(B) by an agency head, as appropriate, for application to the mission critical systems of that agency.

[(2) DEVELOPMENT OF MORE STRINGENT POLICIES, PRINCIPLES, STANDARDS, AND GUIDELINES.—To the extent that such policies are consistent with policies and guidance developed by the Director of the Office of Management and Budget and the Secretary of Commerce, an agency may develop and implement information security policies, principles, standards, and guidelines that provide more stringent protection than those required under section 3533 of title 44, United States Code (as added by section 1061 of this Act), or subsection (a) of this section.

[(g) ATOMIC ENERGY ACT OF 1954.—Nothing in this subtitle (including any amendment made by this subtitle) shall supersede any requirement made by, or under, the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.). Restricted Data or Formerly Restricted Data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).]

ACT OF JANUARY 27, 1938

AN ACT to make confidential certain information furnished to the Bureau of Foreign and Domestic Commerce, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That any statistical information furnished in confidence to the Bureau of Foreign and Domestic Commerce by individuals, corporations, and firms shall be held to be confidential, and shall be used only for the statistical purposes for which it is supplied. [The] *Except as provided in the Confidential Information Protection and Statistical Efficiency Act of 2002, the* Director of the Bureau of Foreign and Domestic Commerce shall not permit anyone other than the sworn employees of the Bureau to examine such individual reports, nor shall he permit any statistics of domestic commerce to be published in such manner as to reveal the identity of the individual, corporation, or firm furnishing such data.

* * * * * * *

CHAPTER 10 OF TITLE 13, UNITED STATES CODE

CHAPTER 10—EXCHANGE OF CENSUS INFORMATION

* * * * * * *

§ 402. Providing business data to Designated Statistical Agencies

The Bureau of the Census may provide business data to the Bureau of Economic Analysis and the Bureau of Labor Statistics ("Designated Statistical Agencies") if such information is required for an authorized statistical purpose and the provision is the subject of a written agreement with that Designated Statistical Agency, or their successors, as defined in the Confidential Information Protection and Statistical Efficiency Act of 2002.

○