

TITLE X--INFORMATION SECURITY

SEC. 1001. 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

'Sec. 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.'

'Sec. 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;

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

`(D) authentication, which means utilizing digital credentials to assure the identity of users and validate their access;

`(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, the function, operation, or use of which--

`(A) involves intelligence activities;

`(B) involves cryptologic activities related to national security;

`(C) involves command and control of military forces;

`(D) involves equipment that is an integral part of a weapon or weapons system; or

`(E) is critical to the direct fulfillment of military or intelligence missions provided that this definition does not apply to a system that is used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications);

`(3) the term `information technology' has the meaning given that term in section 11101 of title 40; and

`(4) the term `information system' 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 includes--

- `(A) computers and computer networks;
- `(B) ancillary equipment;
- `(C) software, firmware, and related procedures;
- `(D) services, including support services; and
- `(E) related resources.'

`Sec. 3533. Authority and functions of the Director

`(a) The Director shall oversee agency information security policies and practices, by--

- `(1) promulgating information security standards under section 11331 of title 40;
- `(2) overseeing the implementation of policies, principles, standards, and guidelines on information security;
- `(3) 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;
- `(4) 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;
- `(5) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303(b)(5) of title 40, to enforce accountability for compliance

with such requirements;

`(6) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3534(b);

`(7) coordinating information security policies and procedures with related information resources management policies and procedures; 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(d)(9) 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 (7) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

`Sec. 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, including--

`(A) mitigating risks associated with such incidents before substantial damage is done; and

`(B) 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, United States Code, (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.

`Sec. 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--

`(1) shall be performed in accordance with generally accepted government auditing standards; and

`(2) may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

`(e) 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.

`(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.

`Sec. 3536. National security systems

`The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency--

`(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;

`(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

`(3) complies with the requirements of this subchapter.

`Sec. 3537. Authorization of appropriations

`There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.

`Sec. 3538. 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 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' 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. National security systems.

`3537. Authorization of appropriations.

`3538. 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(3) of title 44, United States Code.

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

(i) in subsection 2224(b), by striking '(b) OBJECTIVES AND MINIMUM REQUIREMENTS- (1)' and inserting '(b) OBJECTIVES OF THE PROGRAM-';

(ii) in subsection 2224(b), by striking '(2) the program shall at a minimum meet the requirements of section 3534 and 3535 of title 44, United States Code.'; and

(iii) in subsection 2224(c), 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. 1002. MANAGEMENT OF INFORMATION TECHNOLOGY.

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

Sec. 11331. Responsibilities for Federal information systems standards

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

(b) REQUIREMENT TO PRESCRIBE STANDARDS-

(1) IN GENERAL-

(A) REQUIREMENT- Except as provided under paragraph (2), the Director of the Office of Management and Budget shall, on the basis of proposed standards developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3(a)) and in consultation with the Secretary of Homeland Security, promulgate information security standards pertaining to Federal information systems.

(B) REQUIRED STANDARDS- Standards promulgated under subparagraph (A) shall include--

(i) standards that provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology

Act (15 U.S.C. 278g-3(b)); and

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

`(C) REQUIRED STANDARDS BINDING- Information security standards described under subparagraph (B) shall be compulsory and binding.

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

`(c) APPLICATION OF MORE STRINGENT STANDARDS- The head of an agency may employ standards for the cost-effective information security for all operations and assets within or under the supervision of that agency that are more stringent than the standards promulgated by the Director under this section, if such standards--

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

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

`(d) REQUIREMENTS REGARDING DECISIONS BY DIRECTOR-

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

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

(b) CLERICAL AMENDMENT- The table of sections at the beginning of chapter 113 of title 40, United States Code, is amended by striking the item relating to section 11331 and inserting the following:

`11331. Responsibilities for Federal information systems standards.'

SEC. 1003. 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);

`(3) develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems; and

`(4) carry out the responsibilities described in paragraph (3) through the Computer Security Division.

`(b) 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 (including, but not limited to, the Director of the Office of Management and Budget, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, and the Secretary of Homeland Security) to assure--

`(A) use of appropriate information security policies, procedures, and techniques, in order to improve information security and avoid unnecessary and costly duplication of effort; and

`(B) that such standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems and information contained in such systems;

`(2) provide the public with an opportunity to comment on proposed standards and guidelines;

`(3) submit to the Director of the Office of Management and Budget for promulgation under section 11331 of title 40, 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 Act;

`(5) ensure that such standards and guidelines do not require specific technological solutions or products, including any specific hardware or software security solutions;

`(6) ensure that such standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks; and

`(7) use flexible, performance-based standards and guidelines that, to the greatest extent possible, permit the use of off-the-shelf commercially developed information security products.

`(d) 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.

`(e) 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(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 such title.'.

SEC. 1004. 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. 1005. TECHNICAL AND CONFORMING AMENDMENTS.

(a) FEDERAL COMPUTER SYSTEM SECURITY TRAINING AND PLAN-

(1) REPEAL- Section 11332 of title 40, United States Code, is repealed.

(2) CLERICAL AMENDMENT- The table of sections at the beginning of chapter 113 of title 40, United States Code, as amended by striking the item relating to section 11332.

(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 subtitle G of title X (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 title'; and

(ii) by striking the semicolon and inserting a period; and

(C) by striking paragraph (3).

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

`(c) INVENTORY OF INFORMATION SYSTEMS- (1) The head of each agency shall develop and maintain an inventory of the information systems (including 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. 1006. CONSTRUCTION.

Nothing in this Act, or the amendments made by this Act, 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)).