Calendar No. 489

106TH CONGRESS
2D SESSION

S. 1993

[Report No. 106–259]

A BILL

To reform Government information security by strengthening information security practices throughout the Federal Government.

APRIL 10, 2000

Reported with an amendment

Calendar No. 489

106TH CONGRESS
2D SESSION

S. 1993

[Report No. 106–259]

To reform Government information security by strengthening information security practices throughout the Federal Government.

IN THE SENATE OF THE UNITED STATES

NOVEMBER 19, 1999

Mr. THOMPSON (for himself, Mr. LIEBERMAN, Mr. ABRAHAM, Mr. VOINOVICH, Mr. AKAKA, Mr. CLELAND, Ms. COLLINS, Mr. STEVENS, and Mr. HELMS) introduced the following bill; which was read twice and referred to the Committee on Governmental Affairs

APRIL 10, 2000

Reported by Mr. THOMPSON, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

A BILL

To reform Government information security by strengthening information security practices throughout the Federal Government.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Government Information Security Act of 1999''.

SEC. 2. COORDINATION OF FEDERAL INFORMATION POLICY.

Chapter 35 of title 44, United States Code, is amended by inserting at the end the following:

''SUBCHAPTER II—INFORMATION SECURITY

''§ 3531. Purposes

''The purposes of this subchapter are to—

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

''(2)(A) 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; and

''(B) 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; and

''(4) 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) As used in this subchapter 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).

"§ 3533. Authority and functions of the Director

''(a)(1) Consistent with subchapter I, the Director shall establish governmentwide policies for the management of programs that support the cost-effective security of Federal information systems by promoting security as an integral component of each agency's business operations.

''(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;

‘‘(D) continually monitor and evaluate policy; and

‘‘(E) 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. 759 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 coordinate such agencies and coordinate with industry to—

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

"(B) develop voluntary consensus-based standards for security controls, in a manner consistent with section 2(b)(13) of the National Institute of Standards and Technology Act (15 U.S.C. 272(b)(13));

"(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. 759 note; Public Law 100–235; 101 Stat. 1729); and

‘‘(E) related information management laws; and

‘‘(6) take any authorized action 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 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 authority under this section 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 protecting the integrity, confidentiality, and availability of information and information systems supporting agency operations and assets; and

‘‘(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;

‘‘(2) ensure that each senior program manager is responsible for—

‘‘(A) assessing the information security risk associated with the operations and assets of such manager;

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

‘‘(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 program managers 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 program managers, 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 information security provided or managed by another agency.

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

‘‘(A) periodic assessments of information security risks 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 paragraph (1) 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 personnel activities; and

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

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

‘‘(ii) a process for ensuring remedial action to address any deficiencies; and

‘‘(E) 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; and

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

‘‘(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.

‘‘(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 the Paperwork Reduction Act of 1995 (44 U.S.C. 101 note);

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

‘‘(D) 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 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).

“§ 3535. Annual independent evaluation

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

“(2) Each evaluation under this section shall include—

“(A) an assessment of compliance with—

“(i) the requirements of this subchapter; and

“(ii) related information security policies, procedures, standards, and guidelines; and

“(B) tests of the effectiveness of information security control techniques.

“(b)(1) For agencies with Inspectors General appointed under the Inspector General Act of 1978 (5 U.S.C. App.), annual evaluations required under this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency.

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

“(3) An evaluation of agency information security programs and practices performed by the Comptroller General may be in lieu of the evaluation required under this section.

''(c) Not later than March 1, 2001, and every March 1 thereafter, the results of an evaluation required under this section shall be submitted to the Director.

''(d) Each year the Comptroller General shall—

''(1) review the evaluations required under this section and other information security evaluation results; and

''(2) report to Congress regarding the adequacy of agency information programs and practices.

''(e) Agencies and auditors 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.''.

SEC. 3. RESPONSIBILITIES OF CERTAIN AGENCIES.

(a) DEPARTMENT OF COMMERCE.—The Secretary of Commerce, through the National Institute of Standards and Technology and with technical assistance from the National Security Agency, shall—

(1) develop, issue, review, and update standards and guidance for the security of information in Federal computer 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.

(b) DEPARTMENT OF JUSTICE.—The Department of Justice 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) permitted uses of security techniques and technologies.

(c) GENERAL SERVICES ADMINISTRATION.—The General Services Administration shall—

(1) review and update General Services Administration guidance to agencies on addressing security

considerations when acquiring information technology; and

(2) assist agencies in the acquisition of cost-effective security products, services, and incident response capabilities.

(d) OFFICE OF PERSONNEL MANAGEMENT.—The Office of Personnel Management shall—

(1) review and update Office of Personnel Management regulations concerning computer security training for Federal civilian employees; and

(2) assist the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and computer security best practices.

SEC. 4. TECHNICAL AND CONFORMING AMENDMENTS.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended—

(1) in the table of sections—

(A) by inserting after the chapter heading the following:

"SUBCHAPTER I—FEDERAL INFORMATION POLICY";

and

(B) by inserting after the item relating to section 3520 the following:

"SUBCHAPTER II—INFORMATION SECURITY

"Sec.
"3531. Purposes.

and

(2) by inserting before section 3501 the following:

''SUBCHAPTER I—FEDERAL INFORMATION POLICY''.

(b) REFERENCES TO CHAPTER 35.—Chapter 35 of title 44, United States Code, is amended—

(1) in section 3501—

(A) in the matter preceding paragraph (1), by striking ''chapter'' and inserting ''subchapter''; and

(B) in paragraph (11), by striking ''chapter'' and inserting ''subchapter'';

(2) in section 3502, in the matter preceding paragraph (1), by striking ''chapter'' and inserting ''subchapter'';

(3) in section 3503, in subsection (b), by striking ''chapter'' and inserting ''subchapter'';

(4) in section 3504—

(A) in subsection (a)(2), by striking ''chapter'' and inserting ''subchapter'';

(B) in subsection (d)(2), by striking ''chapter'' and inserting ''subchapter''; and

(C) in subsection (f)(1), by striking ''chapter'' and inserting ''subchapter'';

(5) in section 3505—

(A) in subsection (a), in the matter preceding paragraph (1), by striking ''chapter'' and inserting ''subchapter'';

(B) in subsection (a)(2), by striking ''chapter'' and inserting ''subchapter''; and

(C) in subsection (a)(3)(B)(iii), by striking ''chapter'' and inserting ''subchapter'';

(6) in section 3506—

(A) in subsection (a)(1)(B), by striking ''chapter'' and inserting ''subchapter'';

(B) in subsection (a)(2)(A), by striking ''chapter'' and inserting ''subchapter'';

(C) in subsection (a)(2)(B), by striking ''chapter'' and inserting ''subchapter'';

(D) in subsection (a)(3)—

(i) in the first sentence, by striking ''chapter'' and inserting ''subchapter''; and

(ii) in the second sentence, by striking ''chapter'' and inserting ''subchapter'';

(E) in subsection (b)(4), by striking ''chapter'' and inserting ''subchapter'';

(F) in subsection (c)(1), by striking ''chapter, to'' and inserting ''subchapter, to''; and

(G) in subsection (c)(1)(A), by striking ''chapter'' and inserting ''subchapter'';

(7) in section 3507—

(A) in subsection (c)(3)(B), by striking ''chapter'' and inserting ''subchapter'';

(B) in subsection (h)(2)(B), by striking ''chapter'' and inserting ''subchapter'';

(C) in subsection (h)(3), by striking ''chapter'' and inserting ''subchapter'';

(D) in subsection (j)(1)(A)(i), by striking ''chapter'' and inserting ''subchapter'';

(E) in subsection (j)(1)(B), by striking ''chapter'' and inserting ''subchapter''; and

(F) in subsection (j)(2), by striking ''chapter'' and inserting ''subchapter'';

(8) in section 3509, by striking ''chapter'' and inserting ''subchapter'';

(9) in section 3512—

(A) in subsection (a), by striking ''chapter if'' and inserting ''subchapter if''; and

(B) in subsection (a)(1), by striking ''chapter'' and inserting ''subchapter'';

(10) in section 3514—

(A) in subsection (a)(1)(A), by striking ''chapter'' and inserting ''subchapter''; and

(B) in subsection (a)(2)(A)(ii), by striking ''chapter'' and inserting ''subchapter'' each place it appears;

(11) in section 3515, by striking ''chapter'' and inserting ''subchapter'';

(12) in section 3516, by striking ''chapter'' and inserting ''subchapter'';

(13) in section 3517(b), by striking ''chapter'' and inserting ''subchapter'';

(14) in section 3518—

(A) in subsection (a), by striking ''chapter'' and inserting ''subchapter'' each place it appears;

(B) in subsection (b), by striking ''chapter'' and inserting ''subchapter'';

(C) in subsection (c)(1), by striking ''chapter'' and inserting ''subchapter'';

(D) in subsection (c)(2), by striking ''chapter'' and inserting ''subchapter'';

(E) in subsection (d), by striking ''chapter'' and inserting ''subchapter''; and

(F) in subsection (e), by striking ''chapter'' and inserting ''subchapter''; and

~~(15) in section 3520, by striking "chapter" and inserting "subchapter".~~

~~SEC. 5. EFFECTIVE DATE.~~

~~This Act and the amendments made by this Act shall take effect 30 days after the date of enactment of this Act.~~

SECTION 1. SHORT TITLE.

This Act may be cited as the "Government Information Security Act".

SEC. 2. COORDINATION OF FEDERAL INFORMATION POLICY.

Chapter 35 of title 44, United States Code, is amended by inserting at the end the following:

"SUBCHAPTER II—INFORMATION SECURITY

"§ 3531. Purposes

"The purposes of this subchapter are to—

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

"(2)(A) 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; and

"(B) 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; and

"(4) 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) As used in this subchapter the term—

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

"(2) '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 kept secret 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 agency-wide 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 may be delegated—

"(1) to the Secretary of Defense and the Director of Central Intelligence in the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2); and

"(2) in the case of all other Federal information systems, 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)(i) periodic management testing and evaluation of the effectiveness of information security policies and procedures; and

"(ii) a process for ensuring remedial action to address any significant deficiencies; and

"(E) 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 and the Director of Central Intelligence 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 and the Director of Central Intelligence.

"(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 the Paperwork Reduction Act of 1995 (44 U.S.C. 101 note);

"(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 under this section shall include—

"(A) an assessment of compliance with—

"(i) the requirements of this subchapter; and

"(ii) related information security policies, procedures, standards, and guidelines; and

"(B) tests of the effectiveness of information security control techniques.

"(3) The Inspector General or the independent evaluator performing an evaluation under this section including the Comptroller General may use any 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 or the Director of Central Intelligence as appropriate.

"(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.

"(3) An evaluation of agency information security programs and practices performed by the Comptroller General may be in lieu of the evaluation required under this section.

"(c) Not later than 1 year after the date of enactment of this subchapter, and on that date every year thereafter, 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) Each year the Comptroller General shall—

"(1) review the evaluations required under this section and other information security evaluation results; and

"(2) report to Congress regarding the adequacy of agency information programs and practices.

"(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.".

SEC. 3. 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.—Notwithstanding section 3533 of title 44, United States Code (as added by section 2 of this Act), the Secretary of Defense and the Director of Central Intelligence, shall, consistent with their respective authorities—

(1) 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 2 of this Act), that provide more stringent protection than the policies, principles, standards, and guidelines required under section 3533 of such title; and

(2) ensure the implementation of the information security policies, principles, standards, and guidelines described under paragraph (1).

(c) DEPARTMENT OF JUSTICE.—The Department of Justice 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 General Services Administration 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)(E) of title 44, United States Code (as added by section 2 of this Act); and

(B) the acquisition of cost-effective security products, services, and incident response capabilities.

(e) OFFICE OF PERSONNEL MANAGEMENT.—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 com-

puter 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.—Notwithstanding any provision of this Act (including any amendment made by this Act)—

(1) the Secretary of Defense and the Director of Central Intelligence shall develop such policies, principles, procedures, and guidelines for mission critical systems subject to their control;

(2) the policies, principles, procedures, and guidelines developed by the Secretary of Defense and the Director of Central Intelligence 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, to the mission critical systems of all agencies; or

(B) by an agency head, as appropriate, to the mission critical systems of that agency; and

(3) 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 2 of this Act), or subsection (a) of this section.

SEC. 4. TECHNICAL AND CONFORMING AMENDMENTS.

(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended—

(1) in the table of sections—

(A) by inserting after the chapter heading the following:

"SUBCHAPTER I—FEDERAL INFORMATION POLICY";

and

(B) by inserting after the item relating to section 3520 the following:

"SUBCHAPTER II—INFORMATION SECURITY

and

(2) by inserting before section 3501 the following:

"SUBCHAPTER I—FEDERAL INFORMATION POLICY".

(b) REFERENCES TO CHAPTER 35.—Chapter 35 of title 44, United States Code, is amended—

(1) in section 3501—

(A) in the matter preceding paragraph (1), by striking "chapter" and inserting "subchapter"; and

(B) in paragraph (11), by striking "chapter" and inserting "subchapter";

(2) in section 3502, in the matter preceding paragraph (1), by striking "chapter" and inserting "subchapter";

(3) in section 3503, in subsection (b), by striking "chapter" and inserting "subchapter";

(4) in section 3504—

(A) in subsection (a)(2), by striking "chapter" and inserting "subchapter";

(B) in subsection (d)(2), by striking "chapter" and inserting "subchapter"; and

(C) in subsection (f)(1), by striking "chapter" and inserting "subchapter";

(5) in section 3505—

(A) in subsection (a), in the matter preceding paragraph (1), by striking "chapter" and inserting "subchapter";

(B) in subsection (a)(2), by striking "chapter" and inserting "subchapter"; and

(C) in subsection (a)(3)(B)(iii), by striking "chapter" and inserting "subchapter";

(6) in section 3506—

(A) in subsection (a)(1)(B), by striking "chapter" and inserting "subchapter";

(B) in subsection (a)(2)(A), by striking "chapter" and inserting "subchapter";

(C) in subsection (a)(2)(B), by striking "chapter" and inserting "subchapter";

(D) in subsection (a)(3)—

(i) in the first sentence, by striking "chapter" and inserting "subchapter"; and

(ii) in the second sentence, by striking "chapter" and inserting "subchapter";

(E) in subsection (b)(4), by striking "chapter" and inserting "subchapter";

(F) in subsection (c)(1), by striking "chapter, to" and inserting "subchapter, to"; and

(G) in subsection (c)(1)(A), by striking "chapter" and inserting "subchapter";

(7) in section 3507—

(A) in subsection (e)(3)(B), by striking "chapter" and inserting "subchapter";

(B) in subsection (h)(2)(B), by striking "chapter" and inserting "subchapter";

(C) in subsection (h)(3), by striking "chapter" and inserting "subchapter";

(D) in subsection (j)(1)(A)(i), by striking "chapter" and inserting "subchapter";

(E) in subsection (j)(1)(B), by striking "chapter" and inserting "subchapter"; and

(F) in subsection (j)(2), by striking "chapter" and inserting "subchapter";

(8) in section 3509, by striking "chapter" and inserting "subchapter";

(9) in section 3512—

(A) in subsection (a), by striking "chapter if" and inserting "subchapter if"; and

(B) in subsection (a)(1), by striking "chapter" and inserting "subchapter";

(10) in section 3514—

(A) in subsection (a)(1)(A), by striking "chapter" and inserting "subchapter"; and

(B) in subsection (a)(2)(A)(ii), by striking "chapter" and inserting "subchapter" each place it appears;

(11) in section 3515, by striking "chapter" and inserting "subchapter";

(12) in section 3516, by striking "chapter" and inserting "subchapter";

(13) in section 3517(b), by striking "chapter" and inserting "subchapter";

(14) in section 3518—

(A) in subsection (a), by striking "chapter" and inserting "subchapter" each place it appears;

(B) in subsection (b), by striking "chapter" and inserting "subchapter";

(C) in subsection (c)(1), by striking "chapter" and inserting "subchapter";

(D) in subsection (c)(2), by striking "chapter" and inserting "subchapter";

(E) in subsection (d), by striking "chapter" and inserting "subchapter"; and

(F) in subsection (e), by striking "chapter" and inserting "subchapter"; and

(15) in section 3520, by striking "chapter" and inserting "subchapter".

SEC. 5. EFFECTIVE DATE.

This Act and the amendments made by this Act shall take effect 30 days after the date of enactment of this Act.