

106TH CONGRESS
1ST SESSION

S. 1993

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 and Mr. LIEBERMAN) introduced the following bill; which was read twice and referred to the Committee on Governmental Affairs

A BILL

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

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Government Informa-
5 tion Security Act of 1999”.

6 **SEC. 2. COORDINATION OF FEDERAL INFORMATION POL-**
7 **ICY.**

8 Chapter 35 of title 44, United States Code, is amend-
9 ed by inserting at the end the following:

1 “SUBCHAPTER II—INFORMATION SECURITY

2 “§ 3531. Purposes

3 “The purposes of this subchapter are to—

4 “(1) provide a comprehensive framework for es-
5 tablishing and ensuring the effectiveness of controls
6 over information resources that support Federal op-
7 erations and assets;8 “(2)(A) recognize the highly networked nature
9 of the Federal computing environment including the
10 need for Federal Government interoperability and, in
11 the implementation of improved security manage-
12 ment measures, assure that opportunities for inter-
13 operability are not adversely affected; and14 “(B) provide effective governmentwide manage-
15 ment and oversight of the related information secu-
16 rity risks, including coordination of information se-
17 curity efforts throughout the civilian, national secu-
18 rity, and law enforcement communities;19 “(3) provide for development and maintenance
20 of minimum controls required to protect Federal in-
21 formation and information systems; and22 “(4) provide a mechanism for improved over-
23 sight of Federal agency information security pro-
24 grams.

1 **“§ 3532. Definitions**

2 “(a) Except as provided under subsection (b), the
3 definitions under section 3502 shall apply to this sub-
4 chapter.

5 “(b) As used in this subchapter the term ‘information
6 technology’ has the meaning given that term in section
7 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401).

8 **“§ 3533. Authority and functions of the Director**

9 “(a)(1) Consistent with subchapter I, the Director
10 shall establish governmentwide policies for the manage-
11 ment of programs that support the cost-effective security
12 of Federal information systems by promoting security as
13 an integral component of each agency’s business oper-
14 ations.

15 “(2) Policies under this subsection shall—

16 “(A) be founded on a continuing risk manage-
17 ment cycle that recognizes the need to—

18 “(i) identify, assess, and understand risk;

19 and

20 “(ii) determine security needs commensu-
21 rate with the level of risk;

22 “(B) implement controls that adequately ad-
23 dress the risk;

24 “(C) promote continuing awareness of informa-
25 tion security risk;

1 “(D) continually monitor and evaluate policy;
2 and

3 “(E) control effectiveness of information secu-
4 rity practices.

5 “(b) The authority under subsection (a) includes the
6 authority to—

7 “(1) oversee and develop policies, principles,
8 standards, and guidelines for the handling of Fed-
9 eral information and information resources to im-
10 prove the efficiency and effectiveness of govern-
11 mental operations, including principles, policies, and
12 guidelines for the implementation of agency respon-
13 sibilities under applicable law for ensuring the pri-
14 vacy, confidentiality, and security of Federal infor-
15 mation;

16 “(2) consistent with the standards and guide-
17 lines promulgated under section 5131 of the Clinger-
18 Cohen Act of 1996 (40 U.S.C. 1441) and sections
19 5 and 6 of the Computer Security Act of 1987 (40
20 U.S.C. 759 note; Public Law 100–235; 101 Stat.
21 1729), require Federal agencies to identify and af-
22 ford security protections commensurate with the risk
23 and magnitude of the harm resulting from the loss,
24 misuse, or unauthorized access to or modification of

1 information collected or maintained by or on behalf
2 of an agency;

3 “(3) direct the heads of agencies to coordinate
4 such agencies and coordinate with industry to—

5 “(A) identify, use, and share best security
6 practices; and

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

12 “(4) oversee the development and implementa-
13 tion of standards and guidelines relating to security
14 controls for Federal computer systems by the Sec-
15 retary of Commerce through the National Institute
16 of Standards and Technology under section 5131 of
17 the Clinger-Cohen Act of 1996 (40 U.S.C. 1441)
18 and section 20 of the National Institute of Stand-
19 ards and Technology Act (15 U.S.C. 278g-3);

20 “(5) oversee and coordinate compliance with
21 this section in a manner consistent with—

22 “(A) sections 552 and 552a of title 5;

23 “(B) sections 20 and 21 of the National
24 Institute of Standards and Technology Act (15
25 U.S.C. 278g-3 and 278g-4);

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

3 “(D) sections 5 and 6 of the Computer Se-
4 curity Act of 1987 (40 U.S.C. 759 note; Public
5 Law 100–235; 101 Stat. 1729); and

6 “(E) related information management
7 laws; and

8 “(6) take any authorized action that the Direc-
9 tor considers appropriate, including any action in-
10 volving the budgetary process or appropriations
11 management process, to enforce accountability of the
12 head of an agency for information resources man-
13 agement and for the investments made by the agen-
14 cy in information technology, including—

15 “(A) recommending a reduction or an in-
16 crease in any amount for information resources
17 that the head of the agency proposes for the
18 budget submitted to Congress under section
19 1105(a) of title 31;

20 “(B) reducing or otherwise adjusting ap-
21 portionments and reapportionments of appro-
22 priations for information resources; and

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

1 “(c) The authority under this section may be dele-
2 gated only to the Deputy Director for Management of the
3 Office of Management and Budget.

4 **“§ 3534. Federal agency responsibilities**

5 “(a) The head of each agency shall—

6 “(1) be responsible for—

7 “(A) adequately protecting the integrity,
8 confidentiality, and availability of information
9 and information systems supporting agency op-
10 erations and assets; and

11 “(B) developing and implementing infor-
12 mation security policies, procedures, and control
13 techniques sufficient to afford security protec-
14 tions commensurate with the risk and mag-
15 nitude of the harm resulting from unauthorized
16 disclosure, disruption, modification, or destruc-
17 tion of information collected or maintained by
18 or for the agency;

19 “(2) ensure that each senior program manager
20 is responsible for—

21 “(A) assessing the information security
22 risk associated with the operations and assets
23 of such manager;

1 “(B) determining the levels of information
2 security appropriate to protect the operations
3 and assets of such manager; and

4 “(C) periodically testing and evaluating in-
5 formation security controls and techniques;

6 “(3) delegate to the agency Chief Information
7 Officer established under section 3506, or a com-
8 parable official in an agency not covered by such
9 section, the authority to administer all functions
10 under this subchapter including—

11 “(A) designating a senior agency informa-
12 tion security officer;

13 “(B) developing and maintaining an agen-
14 cywide information security program as re-
15 quired under subsection (b);

16 “(C) ensuring that the agency effectively
17 implements and maintains information security
18 policies, procedures, and control techniques;

19 “(D) training and overseeing personnel
20 with significant responsibilities for information
21 security with respect to such responsibilities;
22 and

23 “(E) assisting senior program managers
24 concerning responsibilities under paragraph (2);

1 “(4) ensure that the agency has trained per-
2 sonnel sufficient to assist the agency in complying
3 with the requirements of this subchapter and related
4 policies, procedures, standards, and guidelines; and

5 “(5) ensure that the agency Chief Information
6 Officer, in coordination with senior program man-
7 agers, periodically—

8 “(A)(i) evaluates the effectiveness of the
9 agency information security program, including
10 testing control techniques; and

11 “(ii) implements appropriate remedial ac-
12 tions based on that evaluation; and

13 “(B) reports to the agency head on—

14 “(i) the results of such tests and eval-
15 uations; and

16 “(ii) the progress of remedial actions.

17 “(b)(1) Each agency shall develop and implement an
18 agencywide information security program to provide infor-
19 mation security for the operations and assets of the agen-
20 cy, including information security provided or managed by
21 another agency.

22 “(2) Each program under this subsection shall
23 include—

1 “(A) periodic assessments of information secu-
2 rity risks that consider internal and external threats
3 to—

4 “(i) the integrity, confidentiality, and
5 availability of systems; and

6 “(ii) data supporting critical operations
7 and assets;

8 “(B) policies and procedures that—

9 “(i) are based on the risk assessments re-
10 quired under paragraph (1) that cost-effectively
11 reduce information security risks to an accept-
12 able level; and

13 “(ii) ensure compliance with—

14 “(I) the requirements of this sub-
15 chapter;

16 “(II) policies and procedures as may
17 be prescribed by the Director; and

18 “(III) any other applicable require-
19 ments;

20 “(C) security awareness training to inform per-
21 sonnel of—

22 “(i) information security risks associated
23 with personnel activities; and

1 “(ii) responsibilities of personnel in com-
2 plying with agency policies and procedures de-
3 signed to reduce such risks;

4 “(D)(i) periodic management testing and eval-
5 uation of the effectiveness of information security
6 policies and procedures; and

7 “(ii) a process for ensuring remedial action to
8 address any deficiencies; and

9 “(E) procedures for detecting, reporting, and
10 responding to security incidents, including—

11 “(i) mitigating risks associated with such
12 incidents before substantial damage occurs;

13 “(ii) notifying and consulting with law en-
14 forcement officials and other offices and au-
15 thorities; and

16 “(iii) notifying and consulting with an of-
17 fice designated by the Administrator of General
18 Services within the General Services Adminis-
19 tration.

20 “(3) Each program under this subsection is subject
21 to the approval of the Director and is required to be re-
22 viewed at least annually by agency program officials in
23 consultation with the Chief Information Officer.

1 “(c)(1) Each agency shall examine the adequacy and
2 effectiveness of information security policies, procedures,
3 and practices in plans and reports relating to—

4 “(A) annual agency budgets;

5 “(B) information resources management under
6 the Paperwork Reduction Act of 1995 (44 U.S.C.
7 101 note);

8 “(C) program performance under sections 1105
9 and 1115 through 1119 of title 31, and sections
10 2801 through 2805 of title 39; and

11 “(D) financial management under—

12 “(i) chapter 9 of title 31, United States
13 Code, and the Chief Financial Officers Act of
14 1990 (31 U.S.C. 501 note; Public Law 101–
15 576) (and the amendments made by that Act);

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

20 “(iii) the internal controls conducted under
21 section 3512 of title 31.

22 “(2) Any deficiency in a policy, procedure, or practice
23 identified under paragraph (1) shall be reported as a ma-
24 terial weakness in reporting required under the applicable
25 provision of law under paragraph (1).

1 **“§ 3535. Annual independent evaluation**

2 “(a)(1) Each year each agency shall have an inde-
3 pendent evaluation performed of the information security
4 program and practices of that agency.

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

7 “(A) an assessment of compliance with—

8 “(i) the requirements of this subchapter;

9 and

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

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

14 “(b)(1) For agencies with Inspectors General ap-
15 pointed under the Inspector General Act of 1978 (5
16 U.S.C. App.), annual evaluations required under this sec-
17 tion shall be performed by the Inspector General or by
18 an independent external auditor, as determined by the In-
19 spector General of the agency.

20 “(2) For any agency to which paragraph (1) does not
21 apply, the head of the agency shall contract with an inde-
22 pendent external auditor to perform the evaluation.

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

1 “(c) Not later than March 1, 2001, and every March
2 1 thereafter, the results of an evaluation required under
3 this section shall be submitted to the Director.

4 “(d) Each year the Comptroller General shall—

5 “(1) review the evaluations required under this
6 section and other information security evaluation re-
7 sults; and

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

10 “(e) Agencies and auditors shall take appropriate ac-
11 tions to ensure the protection of information, the disclo-
12 sure of which may adversely affect information security.
13 Such protections shall be commensurate with the risk and
14 comply with all applicable laws.”.

15 **SEC. 3. RESPONSIBILITIES OF CERTAIN AGENCIES.**

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

20 (1) develop, issue, review, and update standards
21 and guidance for the security of information in Fed-
22 eral computer systems, including development of
23 methods and techniques for security systems and
24 validation programs;

1 (2) develop, issue, review, and update guidelines
2 for training in computer security awareness and ac-
3 cepted computer security practices, with assistance
4 from the Office of Personnel Management;

5 (3) provide agencies with guidance for security
6 planning to assist in the development of applications
7 and system security plans for such agencies;

8 (4) provide guidance and assistance to agencies
9 concerning cost-effective controls when inter-
10 connecting with other systems; and

11 (5) evaluate information technologies to assess
12 security vulnerabilities and alert Federal agencies of
13 such vulnerabilities.

14 (b) DEPARTMENT OF JUSTICE.—The Department of
15 Justice shall review and update guidance to agencies on—

16 (1) legal remedies regarding security incidents
17 and ways to report to and work with law enforce-
18 ment agencies concerning such incidents; and

19 (2) permitted uses of security techniques and
20 technologies.

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

23 (1) review and update General Services Admin-
24 istration guidance to agencies on addressing security

1 considerations when acquiring information tech-
2 nology; and

3 (2) assist agencies in the acquisition of cost-ef-
4 fective security products, services, and incident re-
5 sponse capabilities.

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

8 (1) review and update Office of Personnel Man-
9 agement regulations concerning computer security
10 training for Federal civilian employees; and

11 (2) assist the Department of Commerce in up-
12 dating and maintaining guidelines for training in
13 computer security awareness and computer security
14 best practices.

15 **SEC. 4. TECHNICAL AND CONFORMING AMENDMENTS.**

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

18 (1) in the table of sections—

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

“SUBCHAPTER I—FEDERAL INFORMATION POLICY”;

21 and

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

“SUBCHAPTER II—INFORMATION SECURITY

“Sec.

“3531. Purposes.

1 (C) in subsection (f)(1), by striking “chap-
2 ter” and inserting “subchapter”;

3 (5) in section 3505—

4 (A) in subsection (a), in the matter pre-
5 ceding paragraph (1), by striking “chapter”
6 and inserting “subchapter”;

7 (B) in subsection (a)(2), by striking “chap-
8 ter” and inserting “subchapter”; and

9 (C) in subsection (a)(3)(B)(iii), by striking
10 “chapter” and inserting “subchapter”;

11 (6) in section 3506—

12 (A) in subsection (a)(1)(B), by striking
13 “chapter” and inserting “subchapter”;

14 (B) in subsection (a)(2)(A), by striking
15 “chapter” and inserting “subchapter”;

16 (C) in subsection (a)(2)(B), by striking
17 “chapter” and inserting “subchapter”;

18 (D) in subsection (a)(3)—

19 (i) in the first sentence, by striking
20 “chapter” and inserting “subchapter”; and

21 (ii) in the second sentence, by striking
22 “chapter” and inserting “subchapter”;

23 (E) in subsection (b)(4), by striking “chap-
24 ter” and inserting “subchapter”;

1 (F) in subsection (c)(1), by striking “chap-
2 ter, to” and inserting “subchapter, to”; and

3 (G) in subsection (c)(1)(A), by striking
4 “chapter” and inserting “subchapter”;

5 (7) in section 3507—

6 (A) in subsection (e)(3)(B), by striking
7 “chapter” and inserting “subchapter”;

8 (B) in subsection (h)(2)(B), by striking
9 “chapter” and inserting “subchapter”;

10 (C) in subsection (h)(3), by striking “chap-
11 ter” and inserting “subchapter”;

12 (D) in subsection (j)(1)(A)(i), by striking
13 “chapter” and inserting “subchapter”;

14 (E) in subsection (j)(1)(B), by striking
15 “chapter” and inserting “subchapter”; and

16 (F) in subsection (j)(2), by striking “chap-
17 ter” and inserting “subchapter”;

18 (8) in section 3509, by striking “chapter” and
19 inserting “subchapter”;

20 (9) in section 3512—

21 (A) in subsection (a), by striking “chapter
22 if” and inserting “subchapter if”; and

23 (B) in subsection (a)(1), by striking “chap-
24 ter” and inserting “subchapter”;

25 (10) in section 3514—

1 (A) in subsection (a)(1)(A), by striking
2 “chapter” and inserting “subchapter”; and

3 (B) in subsection (a)(2)(A)(ii), by striking
4 “chapter” and inserting “subchapter” each
5 place it appears;

6 (11) in section 3515, by striking “chapter” and
7 inserting “subchapter”;

8 (12) in section 3516, by striking “chapter” and
9 inserting “subchapter”;

10 (13) in section 3517(b), by striking “chapter”
11 and inserting “subchapter”;

12 (14) in section 3518—

13 (A) in subsection (a), by striking “chap-
14 ter” and inserting “subchapter” each place it
15 appears;

16 (B) in subsection (b), by striking “chap-
17 ter” and inserting “subchapter”;

18 (C) in subsection (c)(1), by striking “chap-
19 ter” and inserting “subchapter”;

20 (D) in subsection (c)(2), by striking “chap-
21 ter” and inserting “subchapter”;

22 (E) in subsection (d), by striking “chap-
23 ter” and inserting “subchapter”; and

24 (F) in subsection (e), by striking “chap-
25 ter” and inserting “subchapter”; and

1 (15) in section 3520, by striking “chapter” and
2 inserting “subchapter”.

3 **SEC. 5. EFFECTIVE DATE.**

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

○