

Calendar No. 1105110TH CONGRESS
2^D SESSION**S. 3474**

To amend title 44, United States Code, to enhance information security of the Federal Government, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 11, 2008

Mr. CARPER (for himself, Mr. LIEBERMAN, Ms. COLLINS, and Mr. COLEMAN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

OCTOBER 1 (legislative day, SEPTEMBER 17), 2008

Reported by Mr. LIEBERMAN, without amendment

A BILL

To amend title 44, United States Code, to enhance information security of the Federal Government, and for other purposes.

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 “Federal Information
5 Security Management Act of 2008” or the “FISMA Act
6 of 2008”.

1 **SEC. 2. DEFINITIONS.**

2 Section 3542(b) of title 44, United States Code, is
3 amended by adding at the end the following:

4 “(4) The term ‘adequate security’ means secu-
5 rity commensurate with the risk and magnitude of
6 harm resulting from the loss, misuse, or unauthor-
7 ized access to or modification of information.

8 “(5) The term ‘incident’ means an occurrence
9 that actually or potentially jeopardizes the confiden-
10 tiality, integrity, or availability of an information
11 system or the information the system processes,
12 stores, or transmits or that constitutes a violation or
13 imminent threat of violation of security policies, se-
14 curity procedures, or acceptable use policies.

15 “(6) The term ‘information infrastructure’
16 means the underlying framework that information
17 systems and assets rely on in processing, transmit-
18 ting, receiving, or storing information electroni-
19 cally.”.

20 **SEC. 3. ANNUAL INDEPENDENT AUDIT.**

21 (a) REQUIREMENT FOR AUDIT INSTEAD OF EVALUA-
22 TION.—Section 3545 of title 44, United States Code, is
23 amended—

24 (1) in the section heading, by striking “**EVAL-**
25 **UATION**” and inserting “**AUDIT**” ; and

1 (2) in paragraphs (1) and (2) of subsection (a),
2 by striking “evaluation” and inserting “audit” both
3 places that term appears.

4 (b) ADDITIONAL SPECIFIC REQUIREMENTS FOR AU-
5 DITS.—Section 3545(a) of such title is amended—

6 (1) in paragraph (2)—

7 (A) in subparagraph (A), by striking “sub-
8 set of the agency’s information systems;” and
9 inserting the following: “subset of—

10 “*(i)* the information systems used or
11 operated by the agency; and

12 “*(ii)* the information systems used,
13 operated, or supported on behalf of the
14 agency by a contractor of the agency, any
15 subcontractor (at any tier) of such a con-
16 tractor, or any other entity;”;

17 (B) in subparagraph (B), by striking
18 “and” at the end;

19 (C) in subparagraph (C), by striking the
20 period and inserting “; and”; and

21 (D) by adding at the end the following new
22 subparagraph:

23 “(D) a conclusion as to whether the agen-
24 cy’s information security controls are effective,

1 including an identification of any significant de-
2 ficiencies identified in such controls.”; and

3 (2) by adding at the end the following:

4 “(3) Each audit under this section shall con-
5 form to generally accepted government auditing
6 standards.”.

7 (c) TECHNICAL AND CONFORMING AMENDMENTS.—

8 (1) Each of the following provisions of section
9 3545 of title 44, United States Code, is amended by
10 striking “evaluation” and inserting “audit” each
11 place it appears:

12 (A) Subsection (b)(1).

13 (B) Subsection (b)(2).

14 (C) Subsection (c).

15 (D) Subsection (e)(1).

16 (E) Subsection (e)(2).

17 (2) Section 3545(d) of such title is amended to
18 read as follows:

19 “(d) EXISTING INFORMATION.—The audit required
20 by this section may include consideration of relevant au-
21 dits, evaluations, reports, or other information relating to
22 programs or practices of the applicable agency.”.

23 (3) Section 3545(f) of such title is amended by
24 striking “evaluators” and inserting “auditors”.

1 (4) Section 3545(g)(1) of such title is amended
2 by striking “evaluations” and inserting “audits”.

3 (5) Section 3545(g)(3) of such title is amended
4 by striking “Evaluations” and inserting “Audits”.

5 (6) Section 3543(a)(8)(A) of such title is
6 amended by striking “evaluations” and inserting
7 “audits”.

8 (7) Section 3544(b)(5)(B) of such title is
9 amended by striking “a evaluation” and inserting
10 “an audit, evaluation, report, or other information
11 relating to programs or practices of the applicable
12 agency”.

13 **SEC. 4. CHIEF INFORMATION SECURITY OFFICER AND**
14 **CHIEF INFORMATION SECURITY OFFICER**
15 **COUNCIL.**

16 (a) DELEGATIONS TO CHIEF INFORMATION SECUR-
17 RITY OFFICER.—Section 3544(a) of title 44, United
18 States Code, is amended—

19 (1) in paragraph (3)—

20 (A) in the matter preceding subparagraph

21 (A)—

22 (i) by striking “Chief Information Of-
23 ficer established under section 3506” and
24 inserting “Chief Information Security Offi-
25 cer designated under section 3548”; and

1 (ii) by striking “ensure compliance”
2 and inserting “enforce compliance”;
3 (B) by striking subparagraph (A); and
4 (C) by redesignating subparagraphs (B)
5 through (E) as subparagraphs (A) through (D),
6 respectively;
7 (2) in paragraph (4), by inserting “and
8 cleared” after “trained”; and
9 (3) in paragraph (5), by striking “Chief Infor-
10 mation Officer” and inserting “Chief Information
11 Security Officer”.

12 (b) CHIEF INFORMATION SECURITY OFFICER AND
13 CHIEF INFORMATION SECURITY OFFICER COUNCIL.—
14 Chapter 35 of title 44, United States Code, is amended—

15 (1) by redesignating sections 3548 and 3549 as
16 sections 3553 and 3554, respectively; and

17 (2) by inserting after section 3547 the fol-
18 lowing:

19 **“§ 3548. Chief Information Security Officers**

20 “(a) DESIGNATIONS.—(1) Except as provided under
21 paragraph (2), the head of each agency shall designate
22 a Chief Information Security Officer who with such agency
23 head shall carry out the responsibilities of the agency
24 under this subchapter. An individual may not serve as the
25 Chief Information Officer and the Chief Information Secu-

1 rity Officer for an agency at the same time. The Chief
2 Information Security Officer shall report directly to the
3 Chief Information Officer to carry out such responsibil-
4 ities.

5 “(2) The Secretary of Defense and the Secretary of
6 each military department may each designate Chief Infor-
7 mation Security Officers who with the Secretary making
8 the designation shall carry out the responsibilities of the
9 applicable department under this subchapter. An indi-
10 vidual may not serve as the Chief Information Officer and
11 the Chief Information Security Officer for a department
12 at the same time. The Secretary shall provide for the Chief
13 Information Security Officer to report to the applicable
14 Chief Information Officer to carry out such responsibil-
15 ities. If more than 1 Chief Information Security Officer
16 is designated, the respective duties of the Chief Informa-
17 tion Security Officers shall be clearly delineated.

18 “(b) QUALIFICATIONS AND GENERAL DUTIES.—A
19 Chief Information Security Officer shall—

20 “(1) possess necessary qualifications, including
21 education, professional certifications, training, expe-
22 rience, and the security clearance required to admin-
23 ister the functions described under this subchapter;
24 and

1 “(2) have information security duties as the
2 primary duty of that official.

3 “(c) RESPONSIBILITIES.—A Chief Information Secu-
4 rity Officer for an agency shall have the mission, budget,
5 resources, and authority necessary to—

6 “(1) oversee the establishment and maintenance
7 of an incident response capability that on a contin-
8 uous basis can—

9 “(A) detect, report, respond to, contain, in-
10 vestigate, attribute, and mitigate any network,
11 computer, or data security incident that impairs
12 adequate security, in accordance with policy
13 provided by the Office of Management and
14 Budget, in consultation with the Chief Informa-
15 tion Security Officer Council, and guidance
16 from the National Institute of Standards and
17 Technology;

18 “(B) collaborate with other public and pri-
19 vate sector incident response resources to ad-
20 dress incidents that extend beyond the agency;
21 and

22 “(C) not later than 24 hours after dis-
23 covery of any incident described under subpara-
24 graph (A) unless otherwise directed by policy of
25 the Office of Management and Budget, provide

1 notice to the appropriate supporting informa-
2 tion security operating center, inspector gen-
3 eral, and the United States Computer Emer-
4 gency Readiness Team;

5 “(2) collaborate with the Chief Information Of-
6 ficer to establish, maintain, and update an enter-
7 prise network, system, storage, and security archi-
8 tecture framework documentation to be submitted
9 quarterly to the United States Computer Emergency
10 Readiness Team, that includes—

11 “(A) documentation of how technical, man-
12 agerial, and operational security controls are
13 implemented throughout the agency’s informa-
14 tion infrastructure; and

15 “(B) documentation of how the controls
16 described under subparagraph (A) maintain the
17 appropriate level of confidentiality, integrity,
18 and availability of electronic information and
19 information systems based on National Insti-
20 tute of Standards and Technology guidance and
21 Chief Information Security Officers Council rec-
22 ommended approaches;

23 “(3) ensure that—

24 “(A) risk assessments are conducted on a
25 periodic basis;

1 “(B) penetration tests are conducted com-
2 mensurate with risk (as defined by the National
3 Institute of Standards and Technology) for an
4 agency’s information infrastructure; and

5 “(C) information security vulnerabilities
6 are mitigated in a timely fashion;

7 “(4) ensure that annual information technology
8 security awareness and role-based training for agen-
9 cy employees and contractors is conducted;

10 “(5) create, maintain, and manage an informa-
11 tion security performance measurement system that
12 aligns with agency goals and budget process; and

13 “(6) direct and manage information technology
14 security programs and functions within all subordi-
15 nate agency organizations (including components,
16 bureaus, offices, and other organizations within the
17 agency).

18 “(d) CONTINUOUS TECHNICAL MONITORING FOR
19 MALICIOUS ACTIVITY OF AGENCY NETWORK AND INFOR-
20 MATION SYSTEM.—(1) Each agency shall establish a
21 mechanism that allows the Chief Information Security Of-
22 ficer of the agency to detect, monitor, correlate, and ana-
23 lyze, the security of any information system that is con-
24 nected to the agency’s information infrastructure on a
25 continuous basis through automated monitoring.

1 “(2) The Chief Information Security Officer of an
2 agency shall be responsible for and have the authority to
3 assure that any information system connected to the net-
4 work (directly or indirectly) that does not comply with se-
5 curity policies and standards, or has been compromised,
6 is denied access and use of the agency network until the
7 information system meets or exceeds accepted security
8 policies and standards established by—

9 “(A) the National Institute of Standards and
10 Technology;

11 “(B) the Office of Management and Budget;
12 and

13 “(C) the applicable agency.

14 “(3) After notification to the applicable agency’s
15 Chief Information Officer, the Chief Information Security
16 Officer of an agency may prevent access to any informa-
17 tion system or individual that is using or attempts to use
18 the agency information infrastructure if information secu-
19 rity policies and procedures have not been followed or im-
20 plemented.

21 “(4) If the Chief Information Security Officer recog-
22 nizes a network, computer, or data security incident that
23 impairs adequate security of an interagency information
24 system, the Chief Information Security Officer shall notify
25 the managing agency, agency inspector general, and the

1 United States Computer Emergency Readiness Team
2 within 24 hours after discovery of an incident as defined
3 by policy of the Office of Management and Budget.

4 “(e) OPERATIONAL EVALUATION.—(1) The Chief In-
5 formation Security Officer of an agency in consultation
6 with the agency Chief Information Officer, with rec-
7 ommendations from the Chief Information Security Offi-
8 cers Council and in consultation with the Secretary of
9 Homeland Security and the heads of other appropriate
10 Federal agencies, shall—

11 “(A) establish security control testing protocols
12 that ensure that the information infrastructure of
13 the agency, including contractor information systems
14 operating on behalf of the agency are effectively pro-
15 tected against known vulnerabilities, attacks, and ex-
16 ploitations;

17 “(B) oversee the deployment of such protocols
18 throughout the information infrastructure of the
19 agency; and

20 “(C) update and test such protocols on a recur-
21 ring basis.

22 “(2) After consideration of best practices and rec-
23 ommendations for operational evaluations established by
24 the Chief Information Security Officer Council and in con-
25 sultation with the heads of appropriate agencies, the De-

1 partment of Homeland Security shall no less than annu-
2 ally—

3 “(A) conduct an operational evaluation of the
4 information infrastructure of each agency for known
5 vulnerabilities, attacks, and exploitations of Federal
6 networks on a frequent and recurring basis;

7 “(B) evaluate the ability of each agency to
8 monitor, detect, correlate, analyze, report, and re-
9 spond to breaches in information security policies
10 and practices;

11 “(C) report to the agency head, the Chief Infor-
12 mation Officer, and the Chief Information Security
13 Officer of the applicable agency the findings of the
14 operational evaluation; and

15 “(D) in consultation with the Chief Information
16 Officer and the Chief Information Security Officer
17 of the applicable agency, assist with mitigating ex-
18 ploited vulnerabilities, attacks, and exploitations.

19 “(3) Not later than 30 days after receiving an oper-
20 ational evaluation under paragraph (2), the Chief Infor-
21 mation Security Officer of an agency shall provide the
22 Chief Information Officer and the agency head a plan for
23 addressing recommendations and mitigating
24 vulnerabilities contained in the security reports identified

1 under paragraph (2), including a timeline and budget for
2 implementing such plan.

3 “(f) NATIONAL SECURITY SYSTEMS.—Subsections
4 (c), (d), and (e) shall not apply to any national security
5 system as defined under section 3542(b)(2) so long as that
6 system is evaluated in a manner consistent with processes
7 described under subsection (e)(2) (A) through (D) of this
8 section.

9 **“§ 3549. Chief Information Security Officer Council**

10 “(a) ESTABLISHMENT.—There is established in the
11 executive branch a Chief Information Security Officers
12 Council (in this section referred to as the ‘Council’).

13 “(b) MEMBERSHIP.—The members of the Council
14 shall be full-time senior government employees. The mem-
15 bers shall be as follows:

16 “(1) The Administrator of the Office of Elec-
17 tronic Government of the Office of Management and
18 Budget.

19 “(2) The Chief Information Security Officer of
20 each agency described under section 901(b) of title
21 31.

22 “(3) The Chief Information Security Officer of
23 the Department of the Army, the Department of the
24 Navy, and the Department of the Air Force, if chief

1 information officers have been designated for such
2 departments under section 3506(a)(2)(B).

3 “(4) A representative from the Office of the Di-
4 rector of National Intelligence.

5 “(5) A representative from the United States
6 Strategic Command.

7 “(6) A representative from the United States
8 Computer Emergency Readiness Team.

9 “(7) A representative from the Intelligence
10 Community Incident Response Center.

11 “(8) A representative from the Committee on
12 National Security Systems.

13 “(9) Any other officer or employee of the
14 United States designated by the chairperson.

15 “(c) CO-CHAIRPERSONS AND VICE CHAIRPERSONS.—

16 (1) The Director of the National Cyber Security Center
17 shall act as chairperson of the Council. The Administrator
18 of the Office of Electronic Government of the Office of
19 Management and Budget shall act as co-chairperson of the
20 Council.

21 “(2) The vice chairperson of the Council shall be se-
22 lected by the Council from among its members. The vice
23 chairperson shall serve a 1-year term and may serve mul-
24 tiple terms. The vice chairperson shall serve as a liaison
25 to the Chief Information Officer, Council Committee on

1 National Security Systems, and other councils or commit-
2 tees as appointed by the chairperson.

3 “(d) FUNCTIONS.—(1) The Council shall be the prin-
4 cipal interagency forum for establishing best practices and
5 recommendations for operational evaluations that use at-
6 tack-based testing protocols established under section
7 3548(e).

8 “(2) The Council shall—

9 “(A) share experiences and innovative ap-
10 proaches relating to information sharing and infor-
11 mation security best practices, penetration testing
12 regimes, and incident response mitigation;

13 “(B) promote the development and use of
14 standard performance measures for agency informa-
15 tion security that—

16 “(i) are outcome-based;

17 “(ii) focus on risk management;

18 “(iii) align with the business and program
19 goals of the agency;

20 “(iv) measure improvements in the agency
21 security posture over time; and

22 “(v) reduce burdensome compliance meas-
23 ures;

24 “(C) develop and recommend to the Office of
25 Management and Budget the necessary qualifica-

1 tions to be established for Chief Information Secu-
2 rity Officers to be capable of administering the func-
3 tions described under this subchapter including edu-
4 cation, training, and experience;

5 “(D) enhance information system certification
6 and accreditation processes by establishing a
7 prioritized baseline of information security measures
8 and controls that can be continuously monitored
9 through automated mechanisms; and

10 “(E) submit proposed enhancements to the Of-
11 fice of Management and Budget.

12 **“§ 3550. Requirements for contracts relating to agen-**
13 **cy information and information systems**

14 “(a) IN GENERAL.—(1) Not later than 180 days
15 after the date of enactment of the Federal Information
16 Security Management Act of 2008, the Director of the Of-
17 fice of Management and Budget, in consultation with the
18 Director of the National Institutes of Standards and Tech-
19 nology, shall promulgate information security regulations
20 governing contracts (including task or delivery orders
21 issued pursuant to contracts) between the Federal Govern-
22 ment and any individual, corporation, partnership, organi-
23 zation, or other entity that interfaces with an information
24 system of an agency or collects, stores, operates, or main-
25 tains information on behalf of the agency.

1 “(2) Regulations promulgated under this subsection
2 shall specify requirements concerning—

3 “(A) adequacy and effectiveness of the security
4 of information systems;

5 “(B) the collection and transmission of infor-
6 mation, including personally identifiable information;
7 and

8 “(C) procedures in the event of a security inci-
9 dent.

10 “(b) COMPLIANCE.—Notwithstanding any other pro-
11 vision of law, effective 180 days after the issuance of regu-
12 lations under subsection (a), no agency may enter into a
13 contract (or issue a task or delivery orders under a con-
14 tract), or otherwise enter into an agreement, with an indi-
15 vidual, corporation, partnership, organization, or other en-
16 tity that interfaces with an information system of an agen-
17 cy or collects, stores, operates, or maintains information
18 on behalf of the agency, unless the requirements of the
19 contract or agreement are in compliance with such regula-
20 tions.

21 “(c) SECURITY REQUIREMENTS.—Notwithstanding
22 any other provision of law, effective 3 years after the
23 issuance of regulations under subsection (a), no agency
24 may enter into a contract (or issue a task or delivery order
25 under contract), or otherwise enter into an agreement,

1 with an individual, corporation, partnership, organization,
2 or other entity for commercial off the shelf items, includ-
3 ing hardware and software that does not conform to the
4 security requirements in such regulations.

5 **“§ 3551. Reports to Congress**

6 “(a) ANNUAL REPORTS.—(1) On March 1 of each
7 year, the Department of Homeland Security shall submit
8 a report on operational evaluations and testing protocols
9 to—

10 “(A) the Committee on Homeland Security and
11 Governmental Affairs of the Senate;

12 “(B) the Committee on Oversight and Govern-
13 ment Reform and the Committee on Homeland Se-
14 curity of the House of Representatives;

15 “(C) the Select Committee on Intelligence of
16 the Senate;

17 “(D) the Permanent Select Committee on Intel-
18 ligence of the House of Representatives;

19 “(E) the Government Accountability Office; and

20 “(F) the President’s Council on Integrity and
21 Efficiency and the Executive Council on Integrity
22 and Efficiency.

23 “(2) Each report submitted under this subsection
24 shall—

1 “(A) provide detailed information on the oper-
2 ational evaluations of each agency performed during
3 the preceding fiscal year, the results of such evalua-
4 tions, and any actions that remain to be taken under
5 plans included in corrective action reports under sec-
6 tion 3548(e)(3);

7 “(B) describe the effectiveness of the testing
8 protocols developed under section 3548(e)(1) in miti-
9 gating the risks associated with known
10 vulnerabilities, attacks, and exploitations of the in-
11 formation infrastructure of each agency;

12 “(C) describe the information security posture
13 of the Federal Government, including—

14 “(i) the risks to the confidentiality, integ-
15 rity, and availability of information government-
16 wide; and

17 “(ii) a plan of action and milestones to
18 mitigate the risks governmentwide;

19 “(D) include any recommendations for relevant
20 executive branch action and congressional oversight;
21 and

22 “(E) include an unclassified and classified re-
23 port of the operational evaluation.

24 “(b) SECURITY REPORTS AND CORRECTIVE ACTION
25 REPORTS.—The agency head and inspector general of

1 each agency shall make all information security reports
2 and information security corrective action reports avail-
3 able upon request to—

4 “(1) the Secretary of Homeland Security for
5 purposes of completing the requirements under sub-
6 section (a); and

7 “(2) the Comptroller General of the United
8 States.”.

9 (c) TECHNICAL AND CONFORMING AMENDMENTS.—
10 The table of sections for chapter 35 of title 44, United
11 States Code, is amended by striking the items relating to
12 sections 3548 and 3549 and inserting the following:

“Sec.

“3548. Chief Information Security Officers.

“3549. Chief Information Security Officer Council.

“3550. Requirements for contracts relating to agency information and informa-
tion systems.

“3551. Reports to Congress.

“3552. Authorization of appropriations.

“3553. Effect on existing law.”.

Calendar No. 1105

110TH CONGRESS
2^D SESSION

S. 3474

A BILL

To amend title 44, United States Code, to enhance information security of the Federal Government, and for other purposes.

OCTOBER 1 (legislative day, SEPTEMBER 17), 2008
Reported without amendment