110TH CONGRESS
2D 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 and Mr. LIEBERMAN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

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

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 ''Federal Information Security Management Act of 2008'' or the ''FISMA Act of 2008''.

SEC. 2. DEFINITIONS.

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

''(4) The term 'adequate security' means security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

''(5) The term 'incident' means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

''(6) The term 'information infrastructure' means the underlying framework that information systems and assets rely on in processing, transmitting, receiving, or storing information electronically.''.

SEC. 3. ANNUAL INDEPENDENT AUDIT.

(a) REQUIREMENT FOR AUDIT INSTEAD OF EVALUATION.—Section 3545 of title 44, United States Code, is amended—

(1) in the section heading, by striking ''**EVALUATION**'' and inserting ''**AUDIT**'' ; and

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

(b) ADDITIONAL SPECIFIC REQUIREMENTS FOR AUDITS.—Section 3545(a) of such title is amended—

(1) in paragraph (2)—

(A) in subparagraph (A), by striking ''subset of the agency's information systems;'' and inserting the following: ''subset of—

''(i) the information systems used or operated by the agency; and

''(ii) the information systems used, operated, or supported on behalf of the agency by a contractor of the agency, any subcontractor (at any tier) of such a contractor, or any other entity;'';

(B) in subparagraph (B), by striking ''and'' at the end;

(C) in subparagraph (C), by striking the period and inserting ''; and''; and

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

''(D) a conclusion as to whether the agency's information security controls are effective, including an identification of any significant deficiencies identified in such controls.''; and

(2) by adding at the end the following:

''(3) Each audit under this section shall conform to generally accepted government auditing standards.''.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—

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

(A) Subsection (b)(1).

(B) Subsection (b)(2).

(C) Subsection (c).

(D) Subsection (e)(1).

(E) Subsection (e)(2).

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

''(d) EXISTING INFORMATION.—The audit required by this section may include consideration of relevant audits, evaluations, reports, or other information relating to programs or practices of the applicable agency.''.

(3) Section 3545(f) of such title is amended by striking ''evaluators'' and inserting ''auditors''.

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

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

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

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

SEC. 4. CHIEF INFORMATION SECURITY OFFICER AND CHIEF INFORMATION SECURITY OFFICER COUNCIL.

(a) DELEGATIONS TO CHIEF INFORMATION SECURITY OFFICER.—Section 3544(a) of title 44, United States Code, is amended—

(1) in paragraph (3)—

(A) in the matter preceding subparagraph (A)—

(i) by striking ''Chief Information Officer established under section 3506'' and inserting ''Chief Information Security Officer designated under section 3548''; and

(ii) by striking ''ensure compliance'' and inserting ''enforce compliance'';

(B) by striking subparagraph (A); and

(C) by redesignating subparagraphs (B) through (E) as subparagraphs (A) through (D), respectively;

(2) in paragraph (4), by inserting ''and cleared'' after ''trained''; and

(3) in paragraph (5), by striking ''Chief Information Officer'' and inserting ''Chief Information Security Officer''.

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

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

(2) by inserting after section 3547 the following:

''§ 3548. Chief Information Security Officers

''(a) DESIGNATIONS.—(1) Except as provided under paragraph (2), the head of each agency shall designate a Chief Information Security Officer who with such agency head shall carry out the responsibilities of the agency under this subchapter. An individual may not serve as the Chief Information Officer and the Chief Information Security Officer for an agency at the same time. The Chief Information Security Officer shall report directly to the

Chief Information Officer to carry out such responsibilities.

''(2) The Secretary of Defense and the Secretary of each military department may each designate Chief Information Security Officers who with the Secretary making the designation shall carry out the responsibilities of the applicable department under this subchapter. An individual may not serve as the Chief Information Officer and the Chief Information Security Officer for a department at the same time. The Secretary shall provide for the Chief Information Security Officer to report to the applicable Chief Information Officer to carry out such responsibilities. If more than 1 Chief Information Security Officer is designated, the respective duties of the Chief Information Security Officers shall be clearly delineated.

''(b) QUALIFICATIONS AND GENERAL DUTIES.—A Chief Information Security Officer shall—

''(1) possess necessary qualifications, including education, professional certifications, training, experience, and the security clearance required to administer the functions described under this subchapter; and

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

''(c) RESPONSIBILITIES.—A Chief Information Security Officer for an agency shall have the mission, budget, resources, and authority necessary to—

''(1) oversee the establishment and maintenance of an incident response capability that on a continuous basis can—

''(A) detect, report, respond to, contain, investigate, attribute, and mitigate any network, computer, or data security incident that impairs adequate security, in accordance with policy provided by the Office of Management and Budget, in consultation with the Chief Information Security Officer Council, and guidance from the National Institute of Standards and Technology;

''(B) collaborate with other public and private sector incident response resources to address incidents that extend beyond the agency; and

''(C) not later than 24 hours after discovery of any incident described under subparagraph (A) unless otherwise directed by policy of the Office of Management and Budget, provide notice to the appropriate supporting information security operating center, inspector gen-

eral, and the United States Computer Emergency Readiness Team;

''(2) collaborate with the Chief Information Officer to establish, maintain, and update an enterprise network, system, storage, and security architecture framework documentation to be submitted quarterly to the United States Computer Emergency Readiness Team, that includes—

''(A) documentation of how technical, managerial, and operational security controls are implemented throughout the agency's information infrastructure; and

''(B) documentation of how the controls described under subparagraph (A) maintain the appropriate level of confidentiality, integrity, and availability of electronic information and information systems based on National Institute of Standards and Technology guidance and Chief Information Security Officers Council recommended approaches;

''(3) ensure that—

''(A) risk assessments are conducted on a periodic basis;

''(B) penetration tests are conducted commensurate with risk (as defined by the National

Institute of Standards and Technology) for an agency's information infrastructure; and

''(C) information security vulnerabilities are mitigated in a timely fashion;

''(4) ensure that annual information technology security awareness and role-based training for agency employees and contractors is conducted;

''(5) create, maintain, and manage an information security performance measurement system that aligns with agency goals and budget process; and

''(6) direct and manage information technology security programs and functions within all subordinate agency organizations (including components, bureaus, offices, and other organizations within the agency).

''(d) CONTINUOUS TECHNICAL MONITORING FOR MALICIOUS ACTIVITY OF AGENCY NETWORK AND INFORMATION SYSTEM.—(1) Each agency shall establish a mechanism that allows the Chief Information Security Officer of the agency to detect, monitor, correlate, and analyze, the security of any information system that is connected to the agency's information infrastructure on a continuous basis through automated monitoring.

''(2) The Chief Information Security Officer of an agency shall be responsible for and have the authority to

assure that any information system connected to the network (directly or indirectly) that does not comply with security policies and standards, or has been compromised, is denied access and use of the agency network until the information system meets or exceeds accepted security policies and standards established by—

''(A) the National Institute of Standards and Technology;

''(B) the Office of Management and Budget; and

''(C) the applicable agency.

''(3) After notification to the applicable agency's Chief Information Officer, the Chief Information Security Officer of an agency may prevent access to any information system or individual that is using or attempts to use the agency information infrastructure if information security policies and procedures have not been followed or implemented.

''(4) If the Chief Information Security Officer recognizes a network, computer, or data security incident that impairs adequate security of an interagency information system, the Chief Information Security Officer shall notify the managing agency, agency inspector general, and the United States Computer Emergency Readiness Team

within 24 hours after discovery of an incident as defined by policy of the Office of Management and Budget.

''(e) OPERATIONAL EVALUATION.—(1) The Chief Information Security Officer of an agency in consultation with the agency Chief Information Officer, with recommendations from the Chief Information Security Officers Council and in consultation with the Secretary of Homeland Security and the heads of other appropriate Federal agencies, shall—

''(A) establish security control testing protocols that ensure that the information infrastructure of the agency, including contractor information systems operating on behalf of the agency are effectively protected against known vulnerabilities, attacks, and exploitations;

''(B) oversee the deployment of such protocols throughout the information infrastructure of the agency; and

''(C) update and test such protocols on a recurring basis.

''(2) After consideration of best practices and recommendations for operational evaluations established by the Chief Information Security Officer Council and in consultation with the heads of appropriate agencies, the De-

partment of Homeland Security shall no less than annually—

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

"(B) evaluate the ability of each agency to monitor, detect, correlate, analyze, report, and respond to breaches in information security policies and practices;

"(C) report to the agency head, the Chief Information Officer, and the Chief Information Security Officer of the applicable agency the findings of the operational evaluation; and

"(D) in consultation with the Chief Information Officer and the Chief Information Security Officer of the applicable agency, assist with mitigating exploited vulnerabilities, attacks, and exploitations.

"(3) Not later than 30 days after receiving an operational evaluation under paragraph (2), the Chief Information Security Officer of an agency shall provide the Chief Information Officer and the agency head a plan for addressing recommendations and mitigating vulnerabilities contained in the security reports identified

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

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

''§ 3549. Chief Information Security Officer Council

''(a) ESTABLISHMENT.—There is established in the executive branch a Chief Information Security Officers Council (in this section referred to as the 'Council').

''(b) MEMBERSHIP.—The members of the Council shall be full-time senior government employees. The members shall be as follows:

''(1) The Administrator of the Office of Electronic Government of the Office of Management and Budget.

''(2) The Chief Information Security Officer of each agency described under section 901(b) of title 31.

''(3) The Chief Information Security Officer of the Department of the Army, the Department of the Navy, and the Department of the Air Force, if chief

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

''(4) A representative from the Office of the Director of National Intelligence.

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

''(6) A representative from the United States Computer Emergency Readiness Team.

''(7) A representative from the Intelligence Community Incident Response Center.

''(8) A representative from the Committee on National Security Systems.

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

''(c) CO-CHAIRPERSONS AND VICE CHAIRPERSONS.—(1) The Director of the National Cyber Security Center shall act as chairperson of the Council. The Administrator of the Office of Electronic Government of the Office of Management and Budget shall act as co-chairperson of the Council.

''(2) The vice chairperson of the Council shall be selected by the Council from among its members. The vice chairperson shall serve a 1-year term and may serve multiple terms. The vice chairperson shall serve as a liaison to the Chief Information Officer, Council Committee on

National Security Systems, and other councils or committees as appointed by the chairperson.

''(d) FUNCTIONS.—(1) The Council shall be the principal interagency forum for establishing best practices and recommendations for operational evaluations that use attack-based testing protocols established under section 3548(e).

''(2) The Council shall—

''(A) share experiences and innovative approaches relating to information sharing and information security best practices, penetration testing regimes, and incident response mitigation;

''(B) promote the development and use of standard performance measures for agency information security that—

''(i) are outcome-based;

''(ii) focus on risk management;

''(iii) align with the business and program goals of the agency;

''(iv) measure improvements in the agency security posture over time; and

''(v) reduce burdensome compliance measures;

''(C) develop and recommend to the Office of Management and Budget the necessary qualifica-

tions to be established for Chief Information Security Officers to be capable of administering the functions described under this subchapter including education, training, and experience;

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

''(E) submit proposed enhancements to the Office of Management and Budget.

''§ 3550. Requirements for contracts relating to agency information and information systems

''(a) IN GENERAL.—(1) Not later than 180 days after the date of enactment of the Federal Information Security Management Act of 2008, the Director of the Office of Management and Budget, in consultation with the Director of the National Institutes of Standards and Technology, shall promulgate information security regulations governing contracts (including task or delivery orders issued pursuant to contracts) between the Federal Government and any individual, corporation, partnership, organization, or other entity that interfaces with an information system of an agency or collects, stores, operates, or maintains information on behalf of the agency.

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

''(A) adequacy and effectiveness of the security of information systems;

''(B) the collection and transmission of information, including personally identifiable information; and

''(C) procedures in the event of a security incident.

''(b) COMPLIANCE.—Notwithstanding any other provision of law, effective 180 days after the issuance of regulations under subsection (a), no agency may enter into a contract (or issue a task or delivery orders under a contract), or otherwise enter into an agreement, with an individual, corporation, partnership, organization, or other entity that interfaces with an information system of an agency or collects, stores, operates, or maintains information on behalf of the agency, unless the requirements of the contract or agreement are in compliance with such regulations.

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

with an individual, corporation, partnership, organization, or other entity for commercial off the shelf items, including hardware and software that does not conform to the security requirements in such regulations.

"§ 3551. Reports to Congress

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

''(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

''(B) the Committee on Oversight and Government Reform and the Committee on Homeland Security of the House of Representatives;

''(C) the Select Committee on Intelligence of the Senate;

''(D) the Permanent Select Committee on Intelligence of the House of Representatives;

''(E) the Government Accountability Office; and

''(F) the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency.

''(2) Each report submitted under this subsection shall—

''(A) provide detailed information on the operational evaluations of each agency performed during the preceding fiscal year, the results of such evaluations, and any actions that remain to be taken under plans included in corrective action reports under section 3548(e)(3);

''(B) describe the effectiveness of the testing protocols developed under section 3548(e)(1) in mitigating the risks associated with known vulnerabilities, attacks, and exploitations of the information infrastructure of each agency;

''(C) describe the information security posture of the Federal Government, including—

''(i) the risks to the confidentiality, integrity, and availability of information governmentwide; and

''(ii) a plan of action and milestones to mitigate the risks governmentwide;

''(D) include any recommendations for relevant executive branch action and congressional oversight; and

''(E) include an unclassified and classified report of the operational evaluation.

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

each agency shall make all information security reports and information security corrective action reports available upon request to—

''(1) the Secretary of Homeland Security for purposes of completing the requirements under subsection (a); and

''(2) the Comptroller General of the United States.''.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—The table of sections for chapter 35 of title 44, United States Code, is amended by striking the items relating to 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 information systems.
''3551. Reports to Congress.
''3552. Authorization of appropriations.
''3553. Effect on existing law.''.

○