Union Calendar No. 496

110TH CONGRESS
2D SESSION

H. R. 5983

[Report No. 110–777]

To amend the Homeland Security Act of 2002 to enhance the information security of the Department of Homeland Security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MAY 7, 2008

Mr. LANGEVIN (for himself and Mr. THOMPSON of Mississippi) introduced the following bill; which was referred to the Committee on Homeland Security

JULY 24, 2008

Additional sponsors: Ms. JACKSON-LEE of Texas, Mr. BISHOP of New York, Mr. CARSON, and Ms. HARMAN

JULY 24, 2008

Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

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

[For text of introduced bill, see copy of bill as introduced on May 7, 2008]

A BILL

To amend the Homeland Security Act of 2002 to enhance the information security of the Department of Homeland Security, 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 "Homeland Security Network Defense and Accountability Act of 2008".

SEC. 2. AUTHORITY OF CHIEF INFORMATION OFFICER; QUALIFICATIONS FOR APPOINTMENT.

Section 703(a) of the Homeland Security Act of 2002 (6 U.S.C. 343(a)) is amended—

(1) by inserting before the first sentence the following:

"(1) AUTHORITIES AND DUTIES.—The Secretary shall delegate to the Chief Information Officer such authority necessary for the development, approval, implementation, integration, and oversight of policies, procedures, processes, activities, funding, and systems of the Department relating to the management of information and information infrastructure for the Department, including the management of all related mission applications, information resources, and personnel.

"(2) LINE AUTHORITY.—"; and

(2) by adding at the end the following new paragraphs:

"(3) QUALIFICATIONS FOR APPOINTMENT.—An individual may not be appointed as Chief Information Officer unless the individual has—

"(A) demonstrated ability in and knowledge of information technology and information security; and

"(B) not less than 5 years of executive leadership and management experience in information technology and information security in the public or private sector.

"(4) FUNCTIONS.—The Chief Information Officer shall—

"(A) establish and maintain an incident response team that provides a continuous, real-time capability within the Department of Homeland Security to—

"(i) detect, respond to, contain, investigate, attribute, and mitigate any computer incident, as defined by the National Institute of Standards and Technology, that could violate or pose an imminent threat of violation of computer security policies, acceptable use policies, or standard security practices of the Department; and

"(ii) deliver timely notice of any incident to individuals responsible for information infrastructure of the Department, and

to the United States Computer Emergency Readiness Team;

"(B) establish, maintain, and update a network architecture, including a diagram detailing how security controls are positioned throughout the information infrastructure of the Department to maintain the confidentiality, integrity, availability, accountability, and assurance of electronic information; and

"(C) ensure that vulnerability assessments are conducted on a regular basis for any Department information infrastructure connected to the Internet or another external network, and that vulnerabilities are mitigated in a timely fashion.".

SEC. 3. ATTACK-BASED TESTING PROTOCOLS.

Section 703 of the Homeland Security Act of 2002 (6 U.S.C. 343) is amended by adding at the end the following new subsection:

"(c) ATTACK-BASED TESTING PROTOCOLS.—The Chief Information Officer, in consultation with the Inspector General, the Assistant Secretary for Cybersecurity, and the heads of other appropriate Federal agencies, shall—

"(1) establish security control testing protocols that ensure that the Department's information infra-

structure is effectively protected against known attacks against and exploitations of Federal and contractor information infrastructure;

"(2) oversee the deployment of such protocols throughout the information infrastructure of the Department; and

"(3) update such protocols on a regular basis.".

SEC. 4. INSPECTOR GENERAL REVIEWS OF INFORMATION INFRASTRUCTURE.

Section 703 of the Homeland Security Act of 2002 (6 U.S.C. 343) is further amended by adding at the end the following new subsection:

"(d) INSPECTOR GENERAL REVIEWS.—

"(1) IN GENERAL.—The Inspector General of the Department shall use authority under the Inspector General Act of 1978 (5 App. U.S.C.) to conduct announced and unannounced performance reviews and programmatic reviews of the information infrastructure of the Department to determine the effectiveness of security policies and controls of the Department.

"(2) PERFORMANCE REVIEWS.—Performance reviews under this subsection shall test and validate a system's security controls using the protocols created under subsection (c), beginning not later than 270 days after the date of enactment of the Homeland Se-

curity Network Defense and Accountability Act of 2008.

"(3) PROGRAMMATIC REVIEWS.—Programmatic reviews under this subsection shall—

"(A) determine whether an agency of the Department is complying with policies, processes, and procedures established by the Chief Information Officer; and

"(B) focus on risk assessment, risk management, and risk mitigation, with primary regard to the implementation of best practices such as authentication, access control (including remote access), intrusion detection and prevention, data protection and integrity, and any other controls that the Inspector General considers necessary.

"(4) INFORMATION SECURITY REPORT.—The Inspector General shall submit a security report containing the results of each review under this subsection and prioritized recommendations for improving security controls based on that review, including recommendations regarding funding changes and personnel management, to—

"(A) the Secretary;

"(B) the Chief Information Officer; and

"(C) the head of the Department component that was the subject of the review, and other appropriate individuals responsible for the information infrastructure of such agency.

"(5) CORRECTIVE ACTION REPORT.—

"(A) IN GENERAL.—Within 60 days after receiving a security report under paragraph (4), the head of the Department component that was the subject of the review and the Chief Information Officer shall jointly submit a corrective action report to the Secretary and the Inspector General.

"(B) CONTENTS.—The corrective action report—

"(i) shall contain a plan for addressing recommendations and mitigating vulnerabilities contained in the security report, including a timeline and budget for implementing such plan; and

"(ii) shall note any matters in disagreement between the head of the Department component and the Chief Information Officer.

"(6) REPORTS TO CONGRESS.—

"(A) ANNUAL REPORTS.—In conjunction with the reporting requirements of section 3545 of title 44, United States Code, the Inspector General shall submit an annual report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate—

"(i) summarizing the performance and programmatic reviews performed during the preceding fiscal year, the results of those reviews, and any actions that remain to be taken under plans included in corrective action reports under paragraph (5); and

"(ii) describing the effectiveness of the testing protocols developed under subsection (c) in reducing successful exploitations of the Department's information infrastructure.

"(B) SECURITY REPORTS AND CORRECTIVE ACTION REPORTS.—The Inspector General shall make all security reports and corrective action reports available to any member of the Committee on Homeland Security of the House of Representatives, any member of the Committee

on Homeland Security and Governmental Affairs of the Senate, and the Comptroller General of the United States, upon request.".

SEC. 5. INFORMATION INFRASTRUCTURE DEFINED.

Section 703 of the Homeland Security Act of 2002 (6 U.S.C. 343) is further amended by adding at the end the following:

"(e) INFORMATION INFRASTRUCTURE DEFINED.—In this section, the term 'information infrastructure' means systems and assets used in processing, transmitting, receiving, or storing information electronically.".

SEC. 6. NETWORK SERVICE PROVIDERS.

(a) IN GENERAL.—Subtitle D of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 391 et seq.) is amended by adding at the end the following new section:

"SEC. 836. REQUIREMENTS FOR NETWORK SERVICE PROVIDERS.

"(a) COMPATIBILITY DETERMINATION.—

"(1) IN GENERAL.—Before entering into or renewing a covered contract, the Secretary, acting through the Chief Information Officer, must determine that the contractor has an internal information systems security policy that complies with the Department's information security requirements for risk assessment, risk management, and risk mitigation,

with primary regard to the implementation of best practices such as authentication, access control (including remote access), intrusion detection and prevention, data protection and integrity, and any other policies that the Secretary considers necessary to ensure the security of the Department's information infrastructure.

"(2) LIMITATION ON PUBLIC DISCLOSURES.—The Chief Information Officer shall not disclose to the public any information provided for purposes of such determination, notwithstanding any other provision of Federal, State, or local law, including section 552 of title 5, United States Code.

"(b) CONTRACT REQUIREMENTS REGARDING SECURITY.—The Secretary shall include in each covered contract provisions requiring the contractor to—

"(1) implement and regularly update the internal information systems security policy required under subsection (a);

"(2) maintain the capability to provide contracted services on a continuing and ongoing basis to the Department in the event of unplanned or disruptive event; and

"(3) deliver timely notice of any internal computer incident, as defined by the National Institute of

Standards and Technology, that could violate or pose an imminent threat of violation of computer security policies, acceptable use policies, or standard security practices at the Department, to the United States Computer Emergency Readiness Team and the incident response team established under section 703(a)(4).

"(c) CONTRACT REQUIREMENTS REGARDING SUBCONTRACTING.—The Secretary shall include in each covered contract—

"(1) a requirement that the contractor develop and implement a plan for the award of subcontracts, as appropriate, to small business concerns and disadvantaged business concerns in accordance with other applicable requirements, including the terms of such plan, as appropriate; and

"(2) a requirement that the contractor submit to the Secretary, during performance of the contract, periodic reports describing the extent to which the contractor has complied with such plan, including specification (by total dollar amount and by percentage of the total dollar value of the contract) of the value of subcontracts awarded at all tiers of subcontracting to small business concerns, including socially and economically disadvantaged small businesses con-

cerns, small business concerns owned and controlled by service-disabled veterans, HUBZone small business concerns, small business concerns eligible to be awarded contracts pursuant to section 8(a) of the Small Business Act (15 U.S.C. 637(a)), and Historically Black Colleges and Universities and Hispanic-serving institutions, tribal colleges and universities, and other minority institutions.

"(d) EXISTING CONTRACTS.—The Secretary shall, to the extent practicable under the terms of existing contracts, require each contractor who provides covered information services under a contract in effect on the date of the enactment of the Homeland Security Network Defense and Accountability Act of 2008 to comply with the requirements described in subsection (b).

"(e) DEFINITIONS.—For purposes of this section:

"(1) SOCIALLY AND ECONOMICALLY DISADVANTAGED SMALL BUSINESSES CONCERN, SMALL BUSINESS CONCERN OWNED AND CONTROLLED BY SERVICE-DISABLED VETERANS, AND HUBZONE SMALL BUSINESS CONCERN.—The terms 'socially and economically disadvantaged small businesses concern', 'small business concern owned and controlled by service-disabled veterans', and 'HUBZone small business con-

cern' have the meanings given such terms under the Small Business Act (15 U.S.C. 631 et seq.).

"(2) CONTRACTOR.—The term 'contractor' includes each subcontractor of a contractor.

"(3) COVERED CONTRACT.—The term 'covered contract' means a contract entered into or renewed after the date of the enactment of the Homeland Security Network Defense and Accountability Act of 2008 for the provision of covered information services.

"(4) COVERED INFORMATION SERVICES.—The term 'covered information services' means creation, management, maintenance, control, or operation of information networks or Internet Web sites for the Department.

"(5) HISTORICALLY BLACK COLLEGES AND UNIVERSITIES.—The term 'Historically Black Colleges and Universities' means part B institutions under title III of the Higher Education Act of 1965 (20 U.S.C. 1061).

"(6) HISPANIC-SERVING INSTITUTION.—The term 'Hispanic-serving institution' has the meaning given such term under title V of the Higher Education Act of 1965 (20 U.S.C. 1101a(a)(5)).

"(7) INFORMATION INFRASTRUCTURE.—The term 'information infrastructure' has the meaning that term has under section 703.

"(8) TRIBAL COLLEGES AND UNIVERSITIES.—The term 'tribal colleges and universities' has the meaning given such term under the Tribally Controlled College or University Assistance Act of 1978 (25 U.S.C. 1801 et seq.).".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting after the item relating to section 835 the following new item:

"Sec. 836. Requirements for network service providers.".

(c) REPORT.—Within 90 days after the date of enactment of this Act, the Secretary of Homeland Security shall transmit to the Committee on Homeland Security of the House of Representatives and the Homeland Security and Governmental Affairs Committee of the Senate a report describing—

(1) the progress in implementing requirements issued by the Office of Management and Budget for encryption, authentication, Internet Protocol version 6, and Trusted Internet Connections, including a timeline for completion;

(2) a plan, including an estimated budget and a timeline, to investigate breaches against the Department of Homeland Security's information infrastruc-

ture for purposes of counterintelligence assessment, attribution, and response;

(3) a proposal to increase threat information sharing with cleared and uncleared contractors and provide specialized damage assessment training to private sector information security professionals; and

(4) a process to coordinate the Department of Homeland Security's information infrastructure protection activities.

Union Calendar No. 496

110TH CONGRESS
2D SESSION

H. R. 5983

[Report No. 110–777]

A BILL

To amend the Homeland Security Act of 2002 to enhance the information security of the Department of Homeland Security, and for other purposes.

JULY 24, 2008

Committed to the Committee of the Whole House on the State of the Union and ordered to be printed