AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

110TH CONGRESS
2d Session

HOUSE OF REPRESENTATIVES

REPORT
110–777

HOMELAND SECURITY NETWORK DEFENSE AND ACCOUNTABILITY ACT OF 2008

JULY 24, 2008.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. THOMPSON of Mississippi, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 5983]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred the bill (H.R. 5983) to amend the Homeland Security Act of 2002 to enhance the information security of the Department of Homeland Security, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

	Page
Purpose and Summary	5
Background and Need for Legislation	5
Hearings	5
Committee Consideration	6
Committee Votes	7
Committee Oversight Findings	7
New Budget Authority, Entitlement Authority, and Tax Expenditures	7
Congressional Budget Office Estimate	7
Statement of General Performance Goals and Objectives	8
Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits	9
Federal Mandates Statement	9
Advisory Committee Statement	9
Constitutional Authority Statement	9
Applicability to Legislative Branch	9
Section-by-Section Analysis of the Legislation	9
Changes in Existing Law Made by the Bill, as Reported	12
Committee Correspondence	18

The amendment is as follows:

Strike all after the enacting clause and insert the following:

69–006

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 infrastructure 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 Security 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 concerns, 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 concern' 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 infrastructure 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.

PURPOSE AND SUMMARY

The purpose of H.R. 5983 is to amend the Homeland Security Act of 2002 to enhance the information security of the Department of Homeland Security, and for other purposes.

BACKGROUND AND NEED FOR LEGISLATION

During the course of the 110th Congress, the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology of the Committee on Homeland Security conducted dozens of hearings and investigations into cybersecurity issues affecting Federal and critical infrastructure networks, with the goal of increasing public awareness, fixing vulnerabilities, and holding individuals, agencies, and private sector entities responsible and accountable for their actions. The Committee became particularly concerned with improving the information security posture of the Department of Homeland Security, regarded by many experts—including the Government Accountability Office—as having inadequate security controls in place to safeguard the existing information infrastructure. For instance, during one investigation into the Department's information security practices, the Committee found that weaknesses in security practices resulted in the exfiltration of Departmental data to foreign-language websites. The Committee believes that over time, the theft of critical information from Government servers like those operated by the Department could be harmful to the national and economic security of the United States.

The Committee believes the Department of Homeland Security should be the nation's leader in information security, and seeks to hold the Department to higher standards than other executive agencies through this legislation.

HEARINGS

No hearings were held on H.R. 5983, however the Committee conducted oversight hearings on cybersecurity issues.

On February 15, 2007, the Committee on Homeland Security held a hearing entitled "Lessons Learned and Grading Goals: The Department of Homeland Security in 2007." The Committee received testimony from Michael Jackson, Deputy Secretary, Department of Homeland Security.

On April 19, 2007, the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology held a hearing entitled "Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure." The Subcommittee received testimony from Mr. Greg Wilshusen, Director, Information Security Issues, Government Accountability Office; Mr. Donald Reid, Senior Coordinator for Security Infrastructure, Bureau of Diplomatic Security, Department of State; Mr. Dave Jarrell, Manager, Critical Infrastructure Protection Program, Department of Commerce; Mr. Jerry Dixon, Director, National Cyber Security Division, Department of Homeland Security; Mr. Aaron Turner, Cybersecurity Strategist, National & Homeland Security, Idaho National Laboratory; and Mr. Ken Silva, Chief Security Officer, VeriSign.

On April 25, 2007, the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology held a hearing entitled "Addressing the Nation's Cybersecurity Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action." The Subcommittee received testimony from Dr. Daniel E. Geer, Jr., Principal, Geer Risk Services, LLC; Dr. James Andrew Lewis, Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies; Dr. Douglas Maughan, Program Manager, Cyber Security R&D, science and Technology Directorate, Department of Homeland Security; and Mr. O. Sami Saydjari, President, Professionals for Cyber Defense Chief Executive Officer, Cyber Defense Agency, LLC.

On June 20, 2007, the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology held a hearing entitled "Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security." The Subcommittee received testimony from Mr. Scott Charbo, Chief Information Officer, Department of Homeland Security; Mr. Greg Wilshusen, Director, Information Security Issues, Government Accountability Office; and Mr. Keith A. Rhodes, Chief Technologist, Director, Center for Technology and Engineering, Government Accountability Office.

COMMITTEE CONSIDERATION

H.R. 5983 was introduced in the House by Mr. Langevin and Mr. Thompson of Mississippi on May 7, 2008, and referred solely to the Committee on Homeland Security.

The Committee on Homeland Security considered H.R. 5983 on June 26, 2008, and ordered the measure to be reported to the House favorably, as amended, by voice vote.

The following amendment was offered:

An Amendment in the Nature of a Substitute offered by Mr. Langevin (#1); was AGREED TO by unanimous consent.

COMMITTEE VOTES

Clause 3(b) of Rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during Committee consideration.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of Rule XIII of the Rules of the House of Representatives, the Committee has held oversight hearings and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of Rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 5983, the Homeland Security Network Defense and Accountability Act of 2008, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 10, 2008.

Hon. BENNY G. THOMPSON,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5983, the Homeland Security Network Defense and Accountability Act of 2008.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz.

Sincerely,

ROBERT A. SUNSHINE
(For Peter R. Orszag, Director).

Enclosure.

H.R. 5983—Homeland Security Network Defense and Accountability Act of 2008

Summary: H.R. 5983 would direct the Department of Homeland Security (DHS) to improve the security of its computer networks and increase oversight of contractors that provide network services to the department. Assuming appropriation of the necessary amounts, CBO estimates that implementing H.R. 5983 would cost $163 million over the 2009–2013 period for DHS to hire additional staff to carry out the bill's provisions. Enacting H.R. 5983 would not affect direct spending or revenues.

H.R. 5983 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA)

and would not affect the budgets of state, local, or tribal governments.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 5983 is shown in the following table. The costs of this legislation fall within budget function 750 (administration of justice).

	By fiscal year, in millions of dollars—					
	2009	2010	2011	2012	2013	2009–2013
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Estimated Authorization Level	27	34	34	35	36	166
Estimated Outlays	25	33	34	35	36	163

Basis of estimate: H.R. 5983 would direct DHS to improve the security of its computer networks and increase oversight of contractors that provide network services to the department. The bill would require the department to establish and maintain an incident response team capable of responding at any time to a threat to the security of the department's computers.

Based on information provided by DHS on how the department would likely carry out the bill's provisions, CBO expects that the department would need to hire about 150 additional staff. Additional personnel would be hired by the Chief Information Officer, the Inspector General, and the procurement office. We estimate that annual costs would reach $33 million by 2010, including salaries, benefits, training and support costs, and new hardware and software components.

Estimated intergovernmental and private-sector impact: H.R. 5983 contains no intergovernmental or private-sector mandates as defined in UMRA and would not affect the budgets of state, local, or tribal governments.

Estimate prepared by: Federal Costs: Mark Grabowicz; Impact on State, Local, and Tribal Governments: Burke Doherty; Impact on the Private Sector: Paige Piper/Bach.

Estimate approved by: Theresa Gullo, Deputy Assistant Director for Budget Analysis.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 5983 contains the following general performance goals, and objectives, including outcome related goals and objectives authorized.

This legislation takes a critical step toward improving the cybersecurity posture at the Department of Homeland Security by ensuring a robust defense-in-depth of the Department's information systems, and holding individuals at all levels accountable for mitigating vulnerabilities within the information technology infrastructure. The legislation establishes authorities and qualifications for the Chief Information Officer (CIO) position at the Department, including specific operational security practices for the CIO to implement. The bill also establishes testing protocols, to reduce the number of successful vulnerability exploitations throughout the Department's networks. Finally, the legislation requires the Secretary of the Department of Homeland Security to make determinations

about the security posture of contractors prior to entering into network service agreements with them; create a detailed counter-intelligence plan to investigate all cyber breaches; and report on a program to increase threat information sharing with cleared contractors. Each of these measures will improve the overall information security at the Department.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

In compliance with rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of the rule XXI.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause 1, which grants Congress the power to provide for the common defense of the United States.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section cites the measure as the "Homeland Security Network Defense and Accountability Act of 2008."

Section 2. Authority of CIO and qualifications

This section requires the Secretary to delegate authorities essential for the Chief Information Officer (CIO) to manage the information and information infrastructure for the Department and requires a CIO to possess certain qualifications, including a background in information security and management. The Committee believes the inclusion of professional requirements will provide the Department with requisite expertise for such an important executive position. Similarly, the Committee is concerned that information security has not received the attention it deserves. Therefore,

the Committee directs the CIO to establish and maintain a continuous real-time incident response team, a network architecture with security controls, and regularly perform vulnerability assessments on the infrastructure.

Section 3. Attack-based testing protocols

This section requires the CIO to consult with the Department of Homeland Security Inspector General, the Assistant Secretary for Cybersecurity, and the heads of other appropriate Federal agencies—including, for instance, the Department of Defense and the experienced practitioners at the National Security Agency's Information Assurance Division—to establish security control testing protocols that will protect the Department's information infrastructure against known attacks and exploitations. The Committee is concerned that the Federal Information Security Management Act (FISMA), while bringing much needed public scrutiny to the information security practices across the Federal Government, has not been as effective in curtailing sophisticated attacks against the Federal information infrastructure. Network administrators must be able to identify and mitigate ongoing exploitations of the Department's infrastructure in order to limit the exfiltration of sensitive information out of the Federal government.

The Committee expects this section will transition information security requirements from a paperwork exercise into operational improvements on the enterprise level. The Committee believes the creation and deployment of new testing protocols throughout the Department's infrastructure will help guard against ongoing attacks.

Section 4. Inspector General reviews of information infrastructure

This section requires the Department of Homeland Security Inspector General to conduct announced and unannounced performance and programmatic reviews of the information infrastructure of the Department to determine the effectiveness of security policies and controls. The Committee seeks to expand upon the model that exists at the Department of Energy's Office of Independent Oversight, requiring the Inspector General to conduct performance reviews based on the protocols created by the CIO and other officials in accordance with the previous section and programmatic reviews to determine the extent to which a Department agency is complying with the policies and procedures established by the CIO. It is important to note that these performance and programmatic reviews are in addition to those reports required by FISMA, and are not an alternative to those mandates.

After conducting a performance or programmatic review, the Inspector General will issue a security report containing the results of the review, including recommendations regarding funding and personnel management to the Secretary, the CIO, the head of the Department component subject to the review, and other appropriate individuals who are responsible for information security at these components. Within 60 days of receiving the security report, the head of the Department component subject to the review and the CIO must submit a corrective action report which includes a plan to address the recommendations of the Inspector General and

mitigate the vulnerabilities uncovered during the review. The Committee recognizes that mitigating vulnerabilities requires appropriate plans and budgets, something that only comes from appropriate executive involvement and oversight and which has not been a priority of the Department. The Committee seeks to create accountability among all Department employees, especially executives responsible for information security within their agencies.

Section 5. Requirements for network service providers

This section requires the CIO—prior to entering into or renewing a covered contract—to determine that the contractor's internal information systems security policy complies with the Department's information security requirements. The Committee found that this common private sector best practice often does not occur at the Department; nevertheless, these efforts are vital to reduce vulnerabilities and successful exploitations at the Department, and must become a part of the procurement language. To help identify the most important aspects of information security management, the Committee directs the CIO to focus his review 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 policy that the Secretary considers necessary to secure the Department's information infrastructure. The Committee believes that by ensuring a high level of security of its contractors, the Department can elevate its own security. Furthermore, the provision requiring the contractor to implement and update its own internal information systems security policy will give the Department legal recourse in the event that it wishes to hold contractors liable for security breaches of contractor-owned networks that affect Department information.

This section also requires the Secretary to include in each covered contract, provisions requiring the contractor to deliver timely notice of any internal computer incident that could violate or pose an imminent threat of violation of computer security policies or practices at the Department to the United States Computer Emergency Readiness Teams (US–CERT) and the CIO's incident response team. These practices are designed to ensure situational awareness of the Department and enhance the security of Government-wide networks.

Because the requirements in this section apply only to contracts entered into after the date of enactment, the Secretary is instructed to obtain this information from current contractors to the extent practicable under the terms of existing contracts.

Furthermore, this section requires the Secretary to issue within 90 days of enactment, a report to the appropriate House and Senate Committees 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 infrastructure for the 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's information infrastructure protection activities as required in the recent report by the Office of the Inspector General.

The Committee is alarmed at the Department's lack of progress in implementing encryption and Internet Protocol Version 6 (IPV6) transition requirements, and believes this should be a top priority for the Secretary. In light of the Committee's investigation into data exfiltration out of the Department's networks, the Committee remains concerned that the Department's Office of Security does not have the resources or manpower to develop an agency-wide counter-intelligence plan, and expects to see a comprehensive initiative developed by both the Office of Security and the Chief Information Officer. The Committee expects the Department will develop a program similar to the ongoing initiative between the Department of Defense and the Defense Industrial Base.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italic and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) * * *

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

* * * * * * *

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

* * * * * * *

Subtitle D—Acquisitions

* * * * * * *

Sec. 836. Requirements for network service providers.

* * * * * * *

TITLE VII—MANAGEMENT

* * * * * * *

SEC. 703. CHIEF INFORMATION OFFICER.

(a) IN GENERAL.—

(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.—The Chief Information Officer shall report to the Secretary, or to another official of the Department, as the Secretary may direct.

(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.

* * * * * * *

(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 infrastructure 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.

(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 Security 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.

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

* * * * * * *

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

* * * * * * *

Subtitle D—Acquisitions

* * * * * * *

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 concerns, 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 concern" 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.).

* * * * * * *

HENRY A. WAXMAN, CALIFORNIA,
CHAIRMAN

EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
BRIAN HIGGINS, NEW YORK
JOHN A. YARMUTH, KENTUCKY
BRUCE L. BRALEY, IOWA
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
BETTY McCOLLUM, MINNESOTA
JIM COOPER, TENNESSEE
CHRIS VAN HOLLEN, MARYLAND
PAUL W. HODES, NEW HAMPSHIRE
CHRISTOPHER S. MURPHY, CONNECTICUT
JOHN P. SARBANES, MARYLAND
PETER WELCH, VERMONT
JACKIE SPEIER, CALIFORNIA

COMMITTEE CORRESPONDENCE
ONE HUNDRED TENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5051
FACSIMILE (202) 225–4784
MINORITY (202) 225–5074

www.oversight.house.gov

TOM DAVIS, VIRGINIA,
RANKING MINORITY MEMBER

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
JOHN J. DUNCAN, JR., TENNESSEE
MICHAEL R. TURNER, OHIO
DARRELL E. ISSA, CALIFORNIA
KENNY MARCHANT, TEXAS
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. McHENRY, NORTH CAROLINA
VIRGINIA FOXX, NORTH CAROLINA
BRIAN P. BILBRAY, CALIFORNIA
BILL SALI, IDAHO
JIM JORDAN, OHIO

July 24, 2008

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
H2-176 Ford House Office Building
Washington, DC 20515

Dear Chairman Thompson:

I am writing about H.R. 5983, the Homeland Security Network Defense and Accountability Act of 2008, which the Homeland Security Committee ordered reported to the House on June 26, 2008.

I appreciate your effort to consult with the Committee on Oversight and Government Reform regarding H.R. 5983. In particular, I appreciate your willingness to strike the provision of the bill addressing the Freedom of Information Act and for agreeing to add a rule of construction with regard to application of the Federal Information Management Security Act (FISMA) to the Department of Homeland Security.

In the interest of expediting consideration of H.R. 5983, and in recognition of your efforts to address my concerns, the Oversight Committee will not request a sequential referral of this bill. I would, however, request your support for the appointment of conferees from the Oversight Committee should H.R. 5983 or a similar Senate bill be considered in conference with the Senate.

Moreover, I believe it is important to identify additional provisions in H.R. 5983 that are of particular concern to me.

Specifically, H.R. 5983 creates new responsibilities that might cause confusion with existing requirements under FISMA. Although these requirements do not necessarily contradict FISMA, I am concerned that when the Department seeks to implement these new requirements there may be uncertainty as to which law takes precedence. The unique set of requirements created in H.R. 5983 does not appear to align with current governmentwide requirements.

The Honorable Bennie G. Thompson
July 24, 2008
Page 2

In addition, I am concerned that H.R. 5983 puts too much responsibility with the Department's Inspector General. In my view, primary responsibility for performance reviews and testing should reside with the Department.

Again, thank you for your efforts to address my concerns with H.R. 5983. Although I still have reservations about a few provisions, I look forward to working with you to resolve these maters and develop policies that benefit the federal government as a whole.

This letter should not be construed as a waiver of the Oversight Committee's legislative jurisdiction over subjects addressed in H.R. 5983 that fall within the jurisdiction of the Oversight Committee.

Please include our exchange of letters on this matter in the Homeland Security Committee Report on H.R. 5983 and in the Congressional Record during consideration of this legislation on the House floor.

Sincerely,

Henry A. Waxman
Chairman

cc: Tom Davis
Ranking Minority Member

BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

PETER T. KING, NEW YORK
RANKING MEMBER

One Hundred Tenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

July 24, 2008

The Honorable Henry A. Waxman
Chairman
Committee on Oversight and
Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your letter regarding H.R. 5983, the "Homeland Security Network Defense and Accountability Act of 2008", introduced on May 7, 2008, by Congressman James R. Langevin.

I appreciate your willingness to work cooperatively on this legislation. I acknowledge that H.R. 5983 contains provisions that fall under the jurisdictional interests of the Committee on Oversight and Government Reform. I appreciate your agreement to not seek a sequential referral of this legislation and I acknowledge that your decision to forgo a sequential referral does not waive, alter, or otherwise affect the jurisdiction of the Committee on Oversight and Government Reform.

Further, I recognize that your Committee reserves the right to seek appointment of conferees on the bill for the portions of the bill that are within your jurisdiction, and I agree to support such a request.

I will ensure that this exchange of letters in included in the Committee's report on H.R. 5983 and in the *Congressional Record* during floor consideration of H.R. 5983. I look forward to working with you on this legislation and other matters of great importance to this nation.

Sincerely,

Bennie G. Thompson
Chairman

cc: The Honorable Nancy Pelosi, Speaker
The Honorable Peter T. King, Ranking Member
The Honorable John Sullivan, Parliamentarian

O