

serve as the main point of contact between their component head and the DHS Chief Privacy Officer; draft and review Privacy Impact Assessments and Federal Register notices published by their component; monitor the component's compliance with all applicable Federal privacy laws and regulations; and conduct supervision of programs, regulations, policies, procedures or guidelines to ensure the component's protection of privacy.

As a result, Mr. Speaker, of the committee's oversight and its commitment to the authorization process, this bill would ensure that privacy considerations are integrated into the decision-making process at all of the DHS components.

I urge my colleagues to join me in supporting this legislation that is not only critical to privacy rights, but the security of our country as well.

Mr. Speaker, I reserve the balance of my time.

Mr. BILIRAKIS. Mr. Speaker, I yield myself such time as I may consume.

I rise today in support of H.R. 5170, the Department of Homeland Security Component Privacy Officer Act, sponsored by my committee colleague, Chris Carney.

H.R. 5170 would direct the Secretary of Homeland Security to designate a full-time privacy official within components of the Department. These components include the Transportation Security Administration, Citizenship and Immigration Services, Customs and Border Protection, Immigration and Customs Enforcement, FEMA, the Coast Guard, the Science and Technology Directorate, the Office of Intelligence and Analysis, and NPPD.

The bill provides that each component privacy official will report directly to the Department's Chief Privacy Officer. Each component privacy officer shall have primary responsibility for implementing the Department's privacy policy within its component.

The bill provides for a dual direct report relationship to both the privacy official's component head and the Department's Chief Privacy Officer in carrying out his or her duties.

I think we all can agree that protecting the privacy of our Nation's citizens is of great importance, and that privacy considerations should be integrated into the decision-making process at all DHS components.

□ 1230

I am pleased that the Department has already recognized the importance of privacy protection. In November, 2007, Secretary Chertoff signed a DHS memorandum entitled Designation of Component Level Privacy Officers. This memorandum calls for the designation of full-time component privacy officers at CBP, ICE, FEMA, the Bureau of Citizen and Immigration Services, the Office of Intelligence and Analysis, and the Science and Technology Directorate. Both TSA, US-

VISIT, and the Bureau of Citizen and Immigration Services had their own privacy officials for some time.

H.R. 5170 takes the additional step of statutorily mandating component privacy officials. The approach this bill takes certainly has much merit, though I hope that we can address some of the Department's concerns about the impacts the bill's mandates may have on the ability of the next Secretary to manage the administration of the Department as the legislative process moves on.

Mr. Speaker, having said that, I intend to support H.R. 5170 and encourage all our colleagues to do the same.

Mr. Speaker, I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, I have no further requests for time, and if the gentleman from Florida has no speakers, then I am prepared to close after the gentleman closes.

Mr. BILIRAKIS. Mr. Speaker, before I yield back the balance of my time, I just want to emphasize how important I believe it is for the House to consider both an authorization and appropriations bill for the Department of Homeland Security this year. Every Republican member of the Committee on Homeland Security has signed a letter to the Speaker, Speaker PELOSI, urging her to bring the fiscal year 2009 DHS Appropriations bill, which the Appropriations Committee has already approved, to the floor immediately. And I will add that the chairman has done an outstanding job. We would respectfully renew that request today.

Mr. Speaker, I yield back the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, public trust in the Department's ability to protect personal privacy rights is abysmally low.

Recently, the Department's Inspector General determined that the Science and Technology Directorate's ADVISE program should be cancelled due to privacy concerns. This determination was made after the Department had spent \$42 billion on the program. We also learned that the chief privacy officer was not brought into the process until almost 2 years after the system had been deployed.

This bill would put a privacy officer in the Science and Technology Directorate. Moreover, the Automated Targeting System, which is a Customs and Border Protection program, has been heavily criticized by privacy advocates. Again, this was a program that was operated for some time in the dark without proper safeguards and departmental oversight. Under this bill CBP would get a privacy officer too.

Quite frankly, Mr. Speaker, there has been a litany of DHS programs that have been cancelled, delayed, or discontinued due to privacy concerns. Almost all of these were the products of Department Component Agencies that do not have a privacy officer within their ranks.

H.R. 5170 will ensure that privacy protections and appropriate safeguards are part and parcel of how each component develops its policies and programs.

I urge my colleagues to support this legislation.

Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Mississippi (Mr. THOMPSON) that the House suspend the rules and pass the bill, H.R. 5170, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. BILIRAKIS. Mr. Speaker, I object to the vote on the ground that a quorum is not present and make the point of order that a quorum is not present.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX and the Chair's prior announcement, further proceedings on this motion will be postponed.

The point of no quorum is considered withdrawn.

#### HOMELAND SECURITY NETWORK DEFENSE AND ACCOUNTABILITY ACT OF 2008

Mr. THOMPSON of Mississippi. Mr. Speaker, I move to suspend the rules and pass 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, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5983

*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 infrastructure is effectively protected against known attacks 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, proc-

esses, 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.—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.

“(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 business 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.

#### SEC. 7. RULE OF CONSTRUCTION.

Nothing in this Act shall be construed as affecting in any manner the application of the Federal Information Management Security Act of 2002 (44 U.S.C. 3541 et seq.), to the Department of Homeland Security, including all requirements and deadlines in that Act.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Mississippi (Mr. THOMPSON) and the gentleman from Florida (Mr. BILL-RAKIS) each will control 20 minutes.

The Chair recognizes the gentleman from Mississippi.

#### GENERAL LEAVE

Mr. THOMPSON of Mississippi. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and include extraneous material on the bill under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Mississippi?

There was no objection.

Mr. THOMPSON of Mississippi. Mr. Speaker, I rise in support of this measure and yield myself as much time as I may consume.

Keeping our Federal and critical infrastructure network secure is an issue of national security. The United States and its allies face a significant and growing threat to our information technology systems. The acquisition of our government’s information by outsiders undermines our strength as a Nation. Over time the theft of critical information from government computers could cost the United States our advantage over our adversaries.

This legislation is the result of extensive oversight work undertaken by the chairman of the Subcommittee on Emerging Threats, Science and Technology, Mr. LANGEVIN.

An organization is only as strong as the integrity and reliability of the information that it keeps. H.R. 5983, a piece of the DHS authorization package, seeks to improve cybersecurity at DHS by ensuring that DHS’s defenses of information systems are robust and by holding individuals at all levels accountable for mitigating vulnerabilities.

H.R. 5983, which was approved by voice vote in the committee, Mr. Speaker, is composed of five important provisions:

First, it establishes authorities and qualifications for the Chief Information Officer position at the Department. Through our oversight work, Mr. Speaker, we have observed how lack of an information security background can hamper the CIO’s understanding and ultimately efforts to secure DHS’ networks.

Second, the bill establishes specific operational security practices for the CIO, including a continuous real-time cyber incident response capability, network security architecture, and vulnerability assessments. These are fundamental elements for a comprehensive information security program.

Third, H.R. 5983 establishes testing protocols to reduce the number of vulnerability exploitations throughout the Department’s networks. Time and again we have heard the current Federal information security requirements do not go far enough to actually “operationalize” security to reduce the number of successful attacks. Under H.R. 5983 security will be “operationalized” at DHS, a Federal agency that has a critical homeland security mission and is the receptacle of highly sensitive information.

Fourth, Mr. Speaker, the bill requires the Secretary of Homeland Se-

curity to determine if the internal security policy of a contractor who provides network services to DHS is consistent with the agency’s requirements. This is a standard operating procedure for all private sector companies. It should be also for DHS as well.

Finally, Mr. Speaker, this bill seeks a formal report from the Secretary of Homeland Security on meeting the deadlines established by the Office of Management and Budget for Trusted Internet Connections, encryption and authentication mandates. These are critical for the Department’s efforts to improve information security. It is unclear whether proper deadlines are being met.

I encourage my colleagues to support the Homeland Security Network Defense and Accountability Act of 2008.

HOUSE OF REPRESENTATIVES, COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,

Washington, DC, July 24, 2008.

Hon. BENNIE G. THOMPSON,

Chairman, Committee on Homeland Security, Ford House Office Building, Washington, DC.

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 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 on 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.

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 matters 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.

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON HOMELAND SECURITY,  
Washington, DC, July 24, 2008.

Hon. HENRY A. WAXMAN,  
Chairman, Committee on Oversight and Government Reform, House of Representatives,  
Rayburn House Office Building, Washington, DC.

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 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.

INFORMATION TECHNOLOGY  
ASSOCIATION OF AMERICA,  
Arlington, VA, June 25, 2008.

Hon. JAMES R. LANGEVIN,  
Chairman, the Homeland Security Subcommittee on Emerging Threats, Cybersecurity, Science, and Technology, House of Representatives, Washington, DC.

On behalf of the more than 350 members of the Information Technology Association of America (ITAA), I am writing to express our support for the overall objective of H.R. 5983. As you know, IT AA has long been an outspoken supporter of many Congressional initiatives to improve federal information security practices and we commend the committee's efforts to specifically address information security at the Department of Homeland Security.

We would like to take this opportunity to note that Sec 836(c) has significant requirements to develop and implement plans for the awarding of subcontracts to small businesses and disadvantaged businesses. This is duplicative of existing law and we feel it is unnecessary to require it in the context of this Bill.

Should you have any questions on these comments or our perspective, please feel free to contact Audrey Plonk or Jennifer Kerber. Thank you for your attention to our concerns.

Sincerely,

PHILIP J. BOND,  
President and CEO.

NEW YORK STATE OFFICE OF CYBER  
SECURITY & CRITICAL INFRASTRUCTURE,  
COORDINATION,

Albany, NY, May 30, 2008.

Re House Bill: H.R. 5983.

Hon. BENNIE THOMPSON,  
Chairman, Emerging Threats, Cybersecurity,  
S&T Subcommittee Committee on Homeland  
Security, House of Representatives, Wash-  
ington, DC.

DEAR CHAIRMAN THOMPSON: The New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) supports H.R. 5983, which amends the Homeland Security Act of 2002 to enhance the information security of the Department of Homeland Security.

It is our view that amending the Act to institutionalize the responsibility for ensuring that the Department's information infrastructure is protected from cyber and other threats to the maximum extent practicable is a crucial step in improving the nation's security. All too often the responsibility for securing our cyber infrastructure gets lost in the myriad of operational activities at the expense of security. It is essential that these vital cyber responsibilities are institutionalized if we are to be as cyber prepared as possible.

Thank you for providing CSCIC with an opportunity to comment on this Bill. Please do not hesitate to contact me if you wish to discuss the Bill further as it advances through the legislative process.

Sincerely,

WILLIAM F. PELGRIN.

Mr. Speaker, I reserve the balance of my time.

Mr. BILIRAKIS. Mr. Speaker, I yield myself such time as I may consume.

I rise today in support of H.R. 5983, the Homeland Security Network Defense and Accountability Act, sponsored by my committee colleague Congressman JAMES LANGEVIN.

H.R. 5983 includes several provisions designated to enhance the information security of the Department of Homeland Security and improve oversight of contractors that provide network services to the Department.

Specifically, the bill requires the Chief Information Officer at the Department to have 5 years of executive leadership and information technology experience. The bill also mandates that all contractors and service providers for the Department have compatible information security policies and programs.

Additionally, the bill directs the Department's Inspector General to develop appropriate security protocols for the Department and to annually test various aspects of the Department against these protocols as well as Federal Information Security Management Act requirements. The bill requires procurement officers to review contractors' security postures prior to awarding a contract and directs the Inspector General to conduct both performance and programmatic reviews of the Department's computer network. The bill does not exempt the Department from Federal Information Security Management Act requirements but directs DHS to focus its efforts on elements that will improve its overall security posture.

DHS has expressed some concerns about the potential impact of the

added responsibilities under the bill, particularly on the Department's ability to recruit and retain qualified individuals to fill these important positions. I hope that we can address these concerns as the legislative process moves forward.

Mr. Speaker, I urge all of my colleagues to support passage of H.R. 5983 to strengthen the security of information at the Department.

Mr. Speaker, I reserve the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, I have no further requests for time, and if the gentleman from Florida has no more speakers, then I am prepared to close after the gentleman closes.

Mr. BILIRAKIS. Mr. Speaker, before I yield back the balance of my time, I just want to emphasize how important I believe it is for the House to consider both an authorization and appropriations bill for the Department of Homeland Security this year. Every Republican member of the Committee on Homeland Security has signed a letter to Speaker PELOSI urging her to bring the fiscal year 2009 DHS appropriations bill, which the Appropriations Committee has already approved under the fine leadership of our chairman, and our chairman has done an outstanding job.

And, Mr. Chairman, I want to say something else. You have been so fair to my colleagues and me this year, and I really enjoy serving on your committee.

So if we could get those bills to the floor immediately, my colleagues and I would appreciate it.

Mr. Speaker, I yield back the balance of my time.

Mr. THOMPSON of Mississippi. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, H.R. 5983 is the product of extensive oversight by Chairman LANGEVIN and the other members of the Emerging Threats, Science and Technology Subcommittee.

After hearing from hundreds of experts on how best to improve information security, reviewing best practices in the public and private sectors, and investigating cyber incidents across the public and private sectors, Chairman LANGEVIN authored the Homeland Security Network Defense and Accountability Act.

H.R. 5983 will ensure that a qualified leader serves as the Chief Information Officer and has direction on what specific operational security practices should be implemented to make DHS's information security defenses robust.

□ 1245

This legislation seeks to make DHS the gold standard when it comes to information security. After all, Mr. Speaker, how can DHS legitimately be the lead Federal agency for cybersecurity and infrastructure protection when it doesn't have its own house in order.

I am pleased to include H.R. 5983 in the package of DHS authorization bills that the Committee on Homeland Security has approved on a bipartisan basis. I urge my colleagues to support me in passing this critical piece of legislation.

Mr. LANGEVIN. Mr. Speaker, I rise in strong support of the Homeland Security Network Defense and Accountability Act of 2008, H.R. 5983. The United States and its allies face a significant and growing threat to our information technology, IT, systems and assets, and to the integrity of our information. The acquisition of this information by outsiders threatens to undermine and over time could cost the United States our advantage over our adversaries. This is a critical national security issue that we can no longer ignore.

As chairman of the Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, I have prioritized this issue in the 110th Congress. I have held seven hearings on cybersecurity issues, heard from hundreds of experts on how best to tackle these problems, reviewed information security best practices in the public and private sectors, investigated cyber incidents across the spectrum—from the State and Commerce Departments to our nation's electric grid—and uncovered and assisted law enforcement in investigating breaches at the Department of Homeland Security. It has become clear that an organization is only as strong as the integrity and reliability of the information that it keeps.

The legislation we're considering today represents a critical step toward improving the cybersecurity posture at the Department of Homeland Security by addressing two key issues: ensuring a robust defense-in-depth of our information systems, and holding individuals at all levels accountable for mitigating vulnerabilities.

This measure is composed of several important provisions. First, it establishes authorities and qualifications for the Chief Information Officer, CIO, position at the Department. In a number of hearings, I have heard concerns that the lack of an information security background can hamper the CIO's understanding and efforts to secure the Department's networks. We cannot allow future Presidents to repeat the mistakes made by this Administration in appointing unqualified individuals to this important office.

Second, the bill establishes specific operational security practices for the CIO, including a continuous, real-time cyber incident response capability, a network architecture emphasizing the positioning of security controls, and vulnerability assessments for each external-facing information infrastructure. These are fundamental elements of a comprehensive information security program.

Third, the bill establishes testing protocols to reduce the number of vulnerability exploitations throughout the Department's networks. Time and again we have heard that the Federal Information Security Management Act—or FISMA—does not operationalize security, and does not effectively reduce the number of successful attacks. We must change this, and we can do so by bringing together the heads of appropriate federal agencies to mitigate known attacks against our governmental infrastructure.

The fourth major provision of the bill requires the DHS Secretary to determine if the

internal security policy of a contractor who provides network services to the Department is consistent with the Department's requirements. Again, this is standard operating procedure for all private sector companies; it should be so for the Federal Government as well.

Finally, this bill seeks a formal report from the Secretary on meeting the deadlines established by the Office of Management and Budget, OMB, for Trusted Internet Connections, TIC, encryption and authentication mandates. These are critical for the Department's efforts in information security, and I am not confident that the proper deadlines are being met.

I encourage my colleagues to support the Homeland Security Network Defense and Accountability Act of 2008 and thank Chairman THOMPSON for his leadership in bringing this important measure to the floor.

Mr. THOMPSON of Mississippi. Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentleman from Mississippi (Mr. THOMPSON) that the House suspend the rules and pass the bill, H.R. 5983, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds being in the affirmative, the ayes have it.

Mr. BILIRAKIS. Mr. Speaker, I object to the vote on the ground that a quorum is not present and make the point of order that a quorum is not present.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX and the Chair's prior announcement, further proceedings on this motion will be postponed.

The point of no quorum is considered withdrawn.

#### NEXT GENERATION RADIATION SCREENING ACT OF 2008

Mr. THOMPSON of Mississippi. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5531) to amend the Homeland Security Act of 2002 to clarify criteria for certification relating to advanced spectroscopic portal monitors, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5531

*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 "Next Generation Radiation Screening Act of 2008".*

#### SEC. 2. MEMORANDUM OF UNDERSTANDING REGARDING ADVANCED SPECTROSCOPIC PORTAL MONITORS.

*(a) IN GENERAL.—Title XIX of the Homeland Security Act of 2002 is amended by adding at the end the following new sections:*

#### "SEC. 1908. ADVANCED SPECTROSCOPIC PORTAL MONITORS.

*"(a) FINDINGS.—Congress finds the following:*

*"(1) The consequences of radiological or nuclear terrorism would be catastrophic.*

*"(2) A system such as the Advanced Spectroscopic Portal (ASP) is intended to improve the process of screening passengers and*

*cargo to prevent the illicit transport of radiological and nuclear material.*

*"(3) A system such as the ASP can always be improved, even after it is deployed.*

*"(4) There is no upper limit to the functionality that can be incorporated into an engineering project of this magnitude.*

*"(5) Delaying deployment of the ASP to increase functionality beyond what is minimally required for deployment may limit the ability of the United States to screen passengers and cargo for radiological and nuclear material.*

*"(6) There are operational differences between primary and secondary screening procedures. Consideration should be given to the implication these differences have on the minimum functionality for systems deployed for use in primary and secondary screening procedures.*

*"(b) AGREEMENT ON FUNCTIONALITY OF ADVANCED SPECTROSCOPIC PORTAL MONITORS.—The Director of the Domestic Nuclear Detection Office and the Commissioner of Customs and Border Protection shall enter into an agreement regarding the minimum required functionality for the deployment of ASP by United States Customs and Border Protection (CBP).*

*"(c) REPORT TO CONGRESS.—Not later than 60 days after the date of the enactment of this section, the Secretary shall provide Congress with the signed memorandum of understanding between the Office and CBP.*

#### "SEC. 1909. CRITERIA FOR CERTIFICATION.

*"(a) FINDINGS.—Congress finds the following:*

*"(1) In developing criteria for Advanced Spectroscopic Portal (ASP) performance, special consideration should be given to the unique challenges associated with detecting the presence of illicit radiological or nuclear material that may be masked by the presence of radiation from naturally occurring radioactive material or legitimate radioactive sources such as those associated with medical or industrial use of radiation.*

*"(2) Title IV of division E of the Consolidated Appropriations Act, 2008 (Public Law 110-161) requires the Secretary to submit to Congress a report certifying that 'a significant increase in operational effectiveness will be achieved' with the ASP before 'funds appropriated under this heading shall be obligated for full-scale procurement of Advanced Spectroscopic Portal Monitors', and requires that 'the Secretary shall submit separate and distinct certifications prior to the procurement of Advanced Spectroscopic Portal Monitors for primary and secondary deployment that address the unique requirements for operational effectiveness of each type of deployment'.*

*"(b) SPECIFICATION OF SIGNIFICANT INCREASE IN OPERATIONAL EFFECTIVENESS.—*

*"(1) IN GENERAL.—The Secretary shall, in accordance with the requirements of title IV of division E of the Consolidated Appropriations Act, 2008, and in consultation with the National Academies, develop quantitative metrics that demonstrate any significant increased operational effectiveness (or lack thereof) of deploying the ASP in Primary and Secondary Screening sites, as determined by United States Customs and Border Protection (CBP).*

*"(2) METRICS.—The metrics referred to in paragraph (1) shall include the following:*

*"(A) A quantitative definition of 'significant increase in operational effectiveness'.*

*"(B) All relevant threat materials.*

*"(C) All relevant masking scenarios.*

*"(D) Cost benefit analysis in accordance with the Federal Accounting Standards Advisory Board Generally Accepted Accounting Principles.*

*"(E) Any other measure the Director and the Commissioner determine appropriate.*

*"(c) CONSIDERATION OF EXTERNAL REVIEWS IN THE DECISION TO CERTIFY.—In determining whether or not to certify that the ASP shows a significant increase in operational effectiveness, the Secretary may consider the following:*