

**THE NEED TO STRENGTHEN INFORMATION
SECURITY AT THE DEPARTMENT OF HOMELAND
SECURITY**

HEARING

BEFORE THE

**SUBCOMMITTEE ON MANAGEMENT,
INTEGRATION, AND OVERSIGHT**

OF THE

**COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES**

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

APRIL 14, 2005

Serial No. 109-9

Printed for the use of the Committee on Homeland Security



Available via the World Wide Web: <http://www.gpoaccess.gov/congress/index.html>

U.S. GOVERNMENT PRINTING OFFICE

22-902 PDF

WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON HOMELAND SECURITY

CHRISTOPHER COX, California, *Chairman*

DON YOUNG, Alaska	BENNIE G. THOMPSON, Mississippi
LAMAR S. SMITH, Texas	LORETTA SANCHEZ, California
CURT WELDON, Pennsylvania, <i>Vice Chairman</i>	EDWARD J. MARKEY, Massachusetts
CHRISTOPHER SHAYS, Connecticut	NORMAN D. DICKS, Washington
PETER T. KING, New York	JANE HARMAN, California
JOHN LINDER, Georgia	PETER A. DEFAZIO, Oregon
MARK E. SOUDER, Indiana	NITA M. LOWEY, New York
TOM DAVIS, Virginia	ELEANOR HOLMES NORTON, District of Columbia
DANIEL E. LUNGREN, California	ZOE LOFGREN, California
JIM GIBBONS, Nevada	SHEILA JACKSON-LEE, Texas
ROB SIMMONS, Connecticut	BILL PASCRELL, JR., New Jersey
MIKE ROGERS, Alabama	DONNA M. CHRISTENSEN, U.S. Virgin Islands
STEVAN PEARCE, New Mexico	BOB ETHERIDGE, North Carolina
KATHERINE HARRIS, Florida	JAMES R. LANGEVIN, Rhode Island
BOBBY JINDAL, Louisiana	KENDRICK B. MEEK, Florida
DAVE G. REICHERT, Washington	
MICHAEL MCCAUL, Texas	
CHARLIE DENT, Pennsylvania	

SUBCOMMITTEE ON MANAGEMENT, INTEGRATION, AND OVERSIGHT

MIKE ROGERS, Alabama, *Chairman*

CHRISTOPHER SHAYS, Connecticut	KENDRICK B. MEEK, Florida, <i>Ranking Member</i>
JOHN LINDER, Georgia	EDWARD J. MARKEY, Massachusetts
TOM DAVIS, Virginia	ZOE LOFGREN, California
KATHERINE HARRIS, Florida	SHEILA JACKSON-LEE, Texas
DAVE G. REICHERT, Washington	DONNA M. CHRISTENSEN, U.S. Virgin Islands
MICHAEL MCCAUL, Texas	BENNIE G. THOMPSON, Mississippi <i>Ex Officio</i>
CHARLIE DENT, Pennsylvania	
CHRISTOPHER COX, California <i>Ex Officio</i>	

CONTENTS

	Page
STATEMENTS	
The Honorable Mike Rogers, a Representative in Congress From the State of Alabama, and Chairman, Subcommittee on Management, Integration, and Oversight	1
The Honorable Kendrick B. Meek, a Representative in Congress From the State of Florida, and Ranking Member, Subcommittee on Management, Integration, and Oversight	2
The Honorable Christopher Cox, a Representative in Congress From the State of California, and Chairman, Committee on Homeland Security	21
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security Prepared Statement	3
The Honorable Sheila Jackson-Lee, a Representative in Congress From the State of Texas	19
The Honorable Dave G. Reichert, a Representative in Congress From the State of Washington	18
WITNESSES	
PANEL I	
Mr. Steven I. Cooper, Chief Information Officer, Department of Homeland Security	15
Mr. Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office	
Oral Statement	4
Prepared Statement	5
PANEL II	
Mr. Mark MacCarthy, Senior Vice President, Public Policy Visa U.S.A.	
Oral Statement	23
Prepared Statement	25
Mr. Marc J. Zwillinger, Partner, Sonnenschein Nath & Rosenthal LLP	
Oral Statement	27
Prepared Statement	29

**THE NEED TO STRENGTHEN
INFORMATION SECURITY AT THE
DEPARTMENT OF HOMELAND SECURITY**

Thursday, April 14, 2005

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON MANAGEMENT,
INTEGRATION, AND OVERSIGHT,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 2:38 p.m., in Room 210, Cannon House Office Building, Hon. Mike Rogers [chairman of the subcommittee] presiding.

Present: Representatives Rogers, Cox, Reichert, Jackson-Lee, and Meek.

Mr. ROGERS. [Presiding.] The hearing will come to order.

I would like to first welcome our witnesses today and thank them for taking the time out of their full schedules to be with us on such short notice. The purpose of today's hearing is to review the deficiencies with the Department of Homeland Security's current information security program and what steps need to be taken to improve the overall performance of this program.

The Office of Management and Budget submitted a report dated March 1, 2005, to Congress on how well Federal agencies are doing in complying with the Federal Information Security Management Act of 2002, known as FISMA. Based on this report, last week, the Government Reform Committee, which is chaired by our colleague on this subcommittee, Congressman Tom Davis, issued its latest Federal Computer Security Report Card which gave a grade of D+ to the whole government, but a grade of F to the Department of Homeland Security.

While the report of the Office of Management and Budget recognized some information security improvements in the Department of Homeland Security, the Department received the same failing grade for 2004 that it received for the previous year.

The Department clearly has many challenges facing it, both outside and inside the area of information security. Given the special and unique mission of the Department to utilize sensitive information to protect our country, the area of information security is an area in which the Department should be a good example, not a poor one. The Department needs to do a better job protecting its own information systems while at the same time it protects the information technology infrastructure of the United States against cyberterrorism.

The subcommittee recognizes the Department is implementing a number of initiatives to improve its information security. For example, the Department is working on a baseline inventory of all systems that can currently be categorized as secure systems under FISMA guidelines. The Department is also aiming to complete certification and accreditation of all these information systems by the end of Fiscal Year 2006.

These are steps in the right direction, but the Department needs to do much more to improve its grade from an F. The changes that need to be implemented to maintain a high standard of information security will improve or involve a long-term commitment and significant effort by the Department and the many entities within the Department. They simply must work together to achieve the common goal of department-wide information security.

Now, this is no easy task, given that there are 22 legacy agencies, many of which brought with them their own IT systems. Today, we will discuss the importance of information security programs and the status of implementation at the Department of Homeland Security.

On our first panel, we will hear from a senior official with the Government Accountability Office about current deficiencies in the Department's information security program and what more needs to be done to fix the problem. We also are pleased to have the Department's Chief Information Officer on this panel to answer questions that the Members may have today.

Our second panel will include two experts on what the private sector is doing to secure information systems. Their insights on lessons learned will be helpful as we evaluate what more the Department of Homeland Security needs to do to strengthen its own information security systems.

I once again thank the witnesses for joining us today and look forward to their testimony on this important topic.

And now I yield the floor to my friend and colleague from Florida, Mr. Meek.

Mr. MEEK. Thank you very much, Mr. Chairman.

I want to thank our witnesses for being here today. Over the past couple of months, high-profile invasions into computer systems of prominent data brokerage firms have—firms that have the trust of information security has been broken into, into the national spotlight. The invasions of ChoicePoint and LexisNexis database were not only descriptive, but also was wide-open to full-scale theft of identity theft.

The citizens across the country of the United States are very, very concerned about these revelations that have taken place over recent days. I can tell you that many of the issues that we have to protect, not only in the department but also in the private sector, has a lot to do with American life, commerce, education, governance, and of course, protecting our country.

Imagine that the hijackers or terrorists looking to conceal their identities and the database that they infiltrated. They, also, as it relates to going into—if they were to also go into the Department of Homeland Security, US-VISIT, or Secure Flight program, a single government infiltration could be a disaster.

What protections do we have in place to assure that vital, not only secret, but tracking information, is actually secure? The Federal Information Security Management Act, commonly referred to as FISMA, which was established in 2002, is supposed to assure that all government agencies establish and enforce policies that could keep information secured. FISMA requires federal agencies to secure, not only their information systems, but the information itself.

However, 3 years later, the federal government continues to lag behind the private sector in designing and implementing information systems. In fact, the House Government Reform Committee gave the federal government, which was mentioned earlier, a D+ on security on the most recent federal computer security scorecard. Even though seven agencies received an F, the one given to the Department of Homeland Security for the second year in a row is especially troubling.

How can DHS fulfill its role in leading federal agencies in cybersecurity and also the private sector? Any compromise of that data would be a disaster.

I look forward to hearing from our witnesses as it relates to how we can secure the homeland, not only from the department, but from also from the GAO. I am pretty sure that the findings in this hearing and as this committee moves forth in protecting the real sensitive information of protecting our country will be used—the information that we receive today will be used to protect future generations.

So I look forward to the testimony.

And, Mr. Chairman, I am glad that we were able to schedule this hearing to hear from these witnesses.

PREPARED STATEMENT OF THE HONORABLE BENNIE THOMPSON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MISSISSIPPI, AND RANKING MEMBER, COMMITTEE ON HOMELAND SECURITY

Thank you, Mr. Chairman; Ranking Member Meek. I am pleased to be meeting today to review the Department's efforts to improve the security of its data and systems under the Federal Information Security Management Act, or FISMA.

The Department of Homeland Security is responsible for leading the Federal effort to secure cyberspace. That is why it is essential that the Department have their data and systems security 'house' in order. It is unacceptable that the leader of our Federal cybersecurity efforts received one of the lowest grades on the House Government Reform Committee's 2004 report card on cyber security within federal agencies. The Department must lead by example—how can we expect the private sector to secure its data and systems if the government cannot secure its own.

We have seen what happens when an entity fails to adequately protect the integrity of its data from inappropriate access. The results can be disastrous.

For example, ChoicePoint had business system failures that resulted in the leaking of 145,000 records containing personal private information. Just two days ago, LexisNexis databases were hacked and the reported loss of data now affects ten times the number of consumers than originally thought.

I look forward to today's testimony on how the "real world" is implementing cyber security.

Mr. ROGERS. I thank the Ranking Member for that statement.

I would also remind members that they can submit statements for the record over the next several days.

The Chairman now calls the first panel and recognizes Mr. Greg Wilshusen, Director of Information Security Issues, GAO.

And the Chair also acknowledges the appearance of Mr. Steven Cooper, Chief Information Officer for the Department of Homeland

Security, who is available to answer questions, but I recognize on such short notice was not able to put together a formal statement.

We look forward to hearing your answers to questions.

But, Greg, if you will go ahead and start, I would appreciate it.

**STATEMENT OF MR. GREGORY C. WILSHUSEN, DIRECTOR,
INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNT-
ABILITY OFFICE**

Mr. WILSHUSEN. Mr. Chairman, Ranking Member, I am pleased to be here today to discuss the Department of Homeland Security's efforts to implement the requirements of the Federal Information Security Management Act of 2002, or FISMA.

This act requires the department to develop, document and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets at the department, including those provided or managed by another agency or contractor.

This program is to include eight components, such as periodic assessment of risk and periodic testing and evaluation of controls. FISMA also requires DHS and the inspector general to report each year on efforts to implement this program.

Mr. Chairman, my bottom-line message today is that continued efforts are needed to sustain progress made by the department in implementing the requirements of FISMA. In my testimony today, I will note areas where the department has made progress and those areas where challenges remain.

In its Fiscal Year 2004 report, the department noted that it continued to make significant progress in implementing key information security requirements. For example, it reported that the percentage of its information systems that have been certified and accredited rose 24 percent to 68 percent.

System certification and accreditation is a process by which agency officials authorize systems to operate. It is to include a security assessment of the management, operational, and technical security controls in the system.

As another example, the percentage of employees and contractors who receive security awareness training increased 71 percentage points in the Fiscal Year 2004 to 85 percent overall.

However, the department and the IG also reported several areas where implementing effective information security practices remains a challenge. For example, the IG assessed the quality of the department's certification and accreditation process as poor.

The IG noted that the process was not consistently performed across the department and there were instances where certified and accredited systems lacked key security documents, such as up-to-date security plans, a current risk assessment, and contingency plans. As a result, DHS performance data may not accurately reflect the status of its efforts to implement this requirement.

As another example, the department reported the 79 percent of its systems did not have a tested contingency plan. These plans provide specific instructions for restoring critical systems, business processes, and information in the event of a disruption of service.

The testing of contingency plans is essential to determining whether the plans will function as intended. Without testing, agen-

cies can have only minimal assurance that they will be able to recover their mission-critical systems and processes in the event of an interruption.

In addition, DHS faces other challenges in implementing FISMA requirements. The department is required to have a complete and accurate inventory of its major systems. However, DHS reported that it did not have a complete and accurate inventory in either Fiscal Year 2003 or 2004. Without reliable information on inventories, DHS and the Congress cannot be fully assured of the department's progress in implementing FISMA.

FISMA also requires DHS to develop a process for planning, implementing and documenting remedial actions to address any deficiencies in its information security policies, procedures and practices. However, in its 2004 FISMA report, the IG noted that the seven of nine major organizational elements lacked the documented plan of action and milestones. As a result, the IG could not verify that all IT security weaknesses were included in the plan.

Mr. Chairman, this concludes my opening statement. I look forward to your questions.

[The statement of Mr. Wilshusen follows:]

UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE

INFORMATION SECURITY

Department of Homeland Security Faces Challenges in Fulfilling Statutory Requirements

PREPARED STATEMENT OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES

Mr. Chairman and Members of the Subcommittee: I am pleased to be here today to discuss efforts by the Department of Homeland Security (DHS) to implement requirements of the Federal Information Security Management Act of 2002 (FISMA).¹ For many years, we have reported that poor information security is a widespread problem that has potentially devastating consequences.² Accordingly, since 1997, we have identified information security as a governmentwide high-risk issue in reports to Congress—most recently in January 2005.³ Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that made them vulnerable to attack, Congress passed FISMA, which permanently authorized and strengthened the federal information security program, evaluation, and reporting requirements established for federal agencies. Under FISMA, agencies are to report annually to the Office of Management and Budget (OMB) who issues guidance for that reporting.

In my testimony today, I will summarize the reported status of DHS's implementation of FISMA, including areas of progress and continuing challenges.

In conducting this review, we analyzed and summarized DHS's fiscal year 2003 and 2004 reports to Congress on FISMA implementation. We also reviewed and summarized the fiscal year 2004 FISMA reports for 24 of the largest federal agencies and their Inspectors General (IGs). In addition, we reviewed standards and guidance issued by Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) pursuant to their FISMA responsibilities. Finally, we reviewed OMB's 2004 report to Congress on the implementation of FISMA governmentwide.⁴ We did not validate the accuracy of the data reported by

¹*Federal Information Security Management Act of 2002, Title III, E-Government Act of 2002*, Pub. L. No. 107-347, December 17, 2002.

²GAO, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

³GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January, 2005).

⁴Office of Management and Budget, *Federal Information Security Management Act (FISMA) 2004 Report to Congress* (Washington, D.C.: March 1, 2005).

DHS, the other 23 CFO agencies, or OMB, but did analyze the IGs' fiscal year 2004 FISMA reports to identify any issues related to the accuracy of agency-reported information. We performed our work from October 2004 to March 2005 in accordance with generally accepted government auditing standards. In addition, we continue to perform on-going work on DHS's management of information security.

Results in Brief

DHS has made progress in implementing key federal information security requirements, yet it continues to face challenges in fulfilling the requirements mandated by FISMA. In its fiscal year 2004 report on FISMA implementation, DHS highlights increases in the majority of the key performance measures (developed by OMB to track agency performance in implementing information security requirements), such as the percentage of agency systems reviewed and percentage of employee and contractor personnel who received security awareness training. For example, DHS reported a substantial increase in the percentage of personnel that received security awareness training, rising from 14 percent in fiscal year 2003 to 85 percent in fiscal year 2004. However, DHS continues to face significant challenges in meeting most statutory information security requirements. For example, DHS has yet to develop a complete and accurate inventory or an effective remediation process.

Background

Since the early 1990s, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, without proper safeguards, this widespread interconnectivity also poses significant risks to the government's computer systems and, more importantly, to the critical operations and infrastructures they support.

We recently reported that, while federal agencies showed improvement in addressing information security, they also continued to have significant control weaknesses in federal computer systems that put federal operations and assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at the risk of disruption. The significance of these weaknesses led us to conclude in the audit of the federal government's fiscal year 2004 financial statements⁵ that information security was a material weakness.⁶ Our audits also identified instances of similar types of weaknesses in non-financial systems. Weaknesses continued to be reported in each of the six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation.

To fully understand the significance of the weaknesses we identified, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the degree of risk caused by security weaknesses is high. The weaknesses identified place a broad array of federal operations and assets at risk. For example:

- resources, such as federal payments and collections, could be lost or stolen;
- computer resources could be used for unauthorized purposes or to launch attacks on others;
- sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information could be inappropriately disclosed, browsed, or copied for purposes of industrial espionage or other types of crime;
- critical operations, such as those supporting national defense and emergency services, could be disrupted;
- data could be modified or destroyed for purposes of fraud, identity theft, or disruption; and
- agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

⁵ U.S. Department of the Treasury, *2004 Financial Report of the United States Government* (Washington, D.C.; 2005).

⁶ A material weakness is a condition that precludes the entity's internal control from providing reasonable assurance that misstatements, losses, or noncompliance material in relation to the financial statements or to stewardship information would be prevented or detected on a timely basis.

- Congress and the administration have established specific information security requirements in both law and policy to help protect the information and information systems that support these critical operations and assets.

FISMA Authorized and Strengthened Information Security Requirements

Enacted into law on December 17, 2002, as Title III of the E-Government Act of 2002, FISMA authorized and strengthened information security program, evaluation, and reporting requirements. FISMA assigns specific responsibilities to agency heads, chief information officers, and IGs. It also assigns responsibilities to OMB, which include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security and reviewing at least annually, and approving or disapproving, agency information security programs.

Overall, FISMA requires each agency to develop, document, and implement an agencywide information security program. This program should provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Specifically, this program is to include:

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

FISMA also established a requirement that each agency develop, maintain, and annually update an inventory of major information systems operated by the agency or that are under its control. This inventory is to include an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency.

Each agency is also required to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. Evaluations of non-national security systems are to be performed by the agency IG or by an independent external auditor, while evaluations related to national security systems are to be performed only by an entity designated by the agency head.

The agencies are to report annually to OMB, selected congressional committees, and the Comptroller General on the adequacy of information security policies, procedures, practices, and compliance with FISMA requirements. In addition, agency heads are required to make annual reports of the results of their independent evaluations to OMB. OMB is also required to submit a report to Congress no later than March 1 of each year on agency compliance, including summary of the findings of agencies' independent evaluations.

Other major provisions require NIST to develop, for systems other than national security systems: (1) standards to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category. NIST must also develop a definition and guidelines concerning detection and handling of information security incidents and guidelines, developed in conjunction with the Department of Defense (DOD) and the National Security Agency, for identifying an information system as a national security system.

OMB Reporting Instructions and Guidance Emphasize Performance Measures

Consistent with FISMA requirements, OMB issues guidance agencies on their annual reporting requirements. On August 23, 2004, OMB issued its fiscal year 2004 reporting instructions. The reporting instructions, similar to the 2003 instructions, emphasize strong focus on performance measures and formatted these instructions to emphasize a quantitative response. OMB has developed performance measures in the following areas, including:

- certification and accreditation,⁷
- annual review of agency systems,
- annual review of contractor operations or facilities,
- annual security awareness training for employees and contractors,
- annual specialized training for employees with significant security responsibilities, and
- testing of contingency plans.

Further, OMB provided instructions for continued agency reporting on the status of remediation efforts through plans of action and milestones. Required for all programs and systems where an IT security weakness has been found, these plans list the weaknesses and show estimated resource needs or other challenges to resolving them, key milestones and completion dates, and the status of corrective actions. The plans are to be submitted twice a year. In addition, agencies are to submit quarterly updates that indicate the number of weaknesses for which corrective action was completed on time (including testing), is ongoing and on track to be completed as originally scheduled, or has been delayed, as well as the number of new weaknesses discovered since the last update.

The IGs' reports were to be based on the results of their independent evaluations, including work performed throughout the reporting period (such as financial statements or other audits). While OMB asked the IGs to respond to the same questions as the agencies, it also asked them to assess whether their agency had developed, implemented, and was managing an agencywide plan of actions and milestones. Further, OMB asked the IGs to assess the certification and accreditation process at their agencies. OMB did not request that the IGs validate agency responses to the performance measures. Instead, as part of their independent evaluations of a subset of agency systems, IGs were asked to assess the reliability of the data for those systems that they evaluated.

Recently-created Department of Homeland Security is Large and Complex

In the aftermath of September 11, invigorating the nation's homeland security missions became one of the federal government's most significant challenges. The Homeland Security Act of 2002 created DHS, combining 22 agencies into one department. DHS, with an estimated 170,000 employees, is the third largest government agency. Not since the creation of DOD more than 50 years ago had the government sought an integration and transformation of this magnitude.

GAO designated implementing and transforming DHS as high risk in 2003 because DHS had to transform 22 agencies—several with major management challenges—into one department, and failure to effectively address its management challenges and program risks could have serious consequences for our national security.⁸ DHS combined 22 agencies specializing in various disciplines: law enforcement, border security, biological research, disaster mitigation, and computer security, for instance. Further, DHS oversees a number of non-homeland-security activities, such as the Coast Guard's marine safety responsibilities and the Federal Emergency Management Agency's natural disaster response functions.

DHS has lead responsibility for preventing terrorist attacks in the United States, reducing the vulnerability of the United States to terrorist attacks, and minimizing the damage and assisting in the recovery from attacks that do occur. DHS has five under secretaries with responsibility over directorates for management, science and technology, information analysis and infrastructure protection, border and transportation security, and emergency preparedness and response. In addition, the department has four other organizations that report directly to the Secretary.

DHS uses a variety of major applications and general support systems in support of operational and administrative requirements. In its 2004 FISMA report, DHS stated that it had 395 systems and 61 contractor operations. These systems often

⁷ Certification is a comprehensive process of assessing the level of security risk, identifying security controls needed to reduce risk and maintain it at an acceptable level, documenting security controls in a security plan, and testing controls to ensure they operate as intended. Accreditation is a written decision by an agency management official authorizing operation of a particular information system or group of systems.

⁸ GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January, 2005).

served specific organizations that are now merged with others, resulting in interoperability issues, data management concerns, and incompatible environments or duplicative processes.

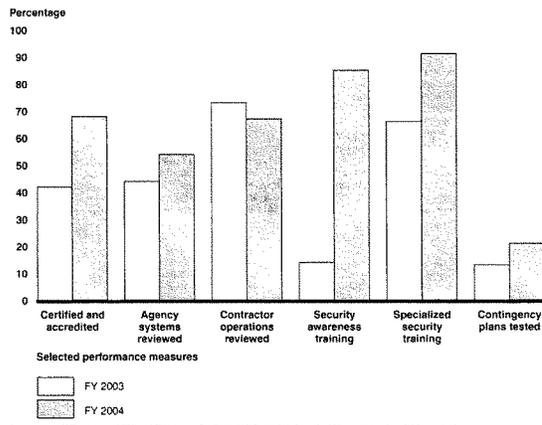
Department of Homeland Security's FISMA Reports Highlight Increases in Performance Measures, but Challenges Remain

In its FISMA-mandated report for fiscal year 2004, DHS generally reported increases in compliance with information security requirements as compared with 2003. However, DHS continues to face significant challenges. The following key performance measures showed increased performance and/or continuing challenges:

- percentage of systems certified and accredited;
- percentage of agency systems reviewed annually;
- percentage of contractor operations reviewed annually;
- percentage of employees and contractors receiving annual security awareness training;
- percentage of employees with significant security responsibilities receiving specialized security training annually; and
- percentage of systems with contingency plans tested.

Figure 1 illustrates the reported overall status of DHS in meeting these performance measures and the changes between fiscal years 2003 and 2004.

Figure 1: DHS Reported Data for Key Performance Measures

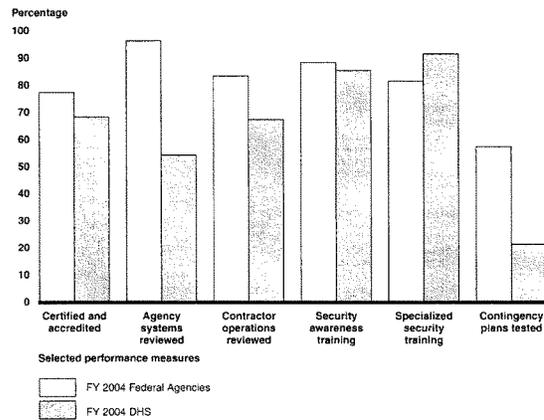


Sources: DHS' FY2003 and FY2004 Report on the Federal Information Security Management Act; GAO (analysis).

DHS has yet to develop a complete and accurate inventory, or an effective plan of action and milestones.⁹ Finally, figure 2 illustrates how DHS compares to the governmentwide results for the performance measures when compared to the aggregated data of all 24 CFO agencies.

⁹OMB's implementing guidance refers to the process of planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security as a security plan of action and milestones.

Figure 2: Comparison of DHS Data to Governmentwide Performance



Sources: OMB's FY2004 Report to Congress on the Federal Information Security Management Act and DHS' FY2004 Report on the Federal Information Security Management Act; GAO (analysis).

Certification and Accreditation

Included in OMB's policy for federal information security is a requirement that agency management officials formally authorize their information systems to process information and, thereby, accept the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan. In 2003, agencies were required to report separately on risk assessments and security plans. In 2004, OMB eliminated this separate reporting in its guidance and directed agencies to complete risk assessments and security plans for the certification and accreditation process to be accomplished. As a result, the performance measure for certification and accreditation now also

reflects the level of agency compliance for risk assessments and security plans. For FISMA reporting, OMB requires agencies to report the number of systems authorized for processing after completing certification and accreditation.

DHS reported a significant increase for this performance measure in its fiscal year 2004 report. The Department reported that approximately 68 percent of its systems had been certified and accredited, an increase of 26 percent over fiscal year 2003. Governmentwide, 77 percent of all systems were certified and accredited compared to the 68 percent at DHS. If agencies do not certify and accredit their systems, they cannot be assured that risks have been identified and mitigated to an acceptable level.

Moreover, the DHS IG reported in its 2004 FISMA report that the certification and accreditation process at the Department was poor. The report noted that the certification and accreditation process was not performed consistently across the Department. In addition, there were instances where certified and accredited systems lacked key security documentation such as up-to-date and approved security plans, a current risk assessment, and contingency plans. As a result, the agency reported performance data may not accurately reflect the status of DHS's efforts to implement this requirement.

Annual Review of Agency Systems

FISMA requires that agency information security programs include periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices to be performed with a frequency that depends on risk, but no less than annually. This is to include testing of management, operational, and technical controls for every information system identified in the FISMA-required inventory of major systems. Periodically evaluating the effectiveness of security policies and controls and acting to address any identified weaknesses are fundamental activities that allow an organization to manage its information security risks cost effectively, rather than reacting to individual problems ad hoc only after a violation has been detected or an audit finding has been reported. Further, management control testing and evaluation as part of program reviews is an additional source of information that can be considered along with control testing and evaluation in IG and GAO audits to help provide a more complete picture of the agencies' security postures. As a performance measure for this requirement, OMB requires that agencies report the number of systems that they have reviewed during the year.

DHS reported performing an annual review on an increased percentage of its systems. It reported in 2004 that it had reviewed 54 percent of its systems, as compared to 44 percent in 2003. In 2004, 23 of the 24 CFO agencies reported that they had reviewed 90 percent or more of their systems. Annual security testing helps to provide assurance to the agencies that security controls are in place and functioning correctly. Without such testing, agencies cannot be assured that their information and systems are protected.

Annual Review of Contractor Operations

Under FISMA, agency heads are responsible for providing information security protections for information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor. Thus, agency information security programs apply to all organizations that possess or use federal information or that operate, use, or have access to federal information systems on behalf of a federal agency. Other such organizations may include contractors, grantees, state and local governments, and industry partners. This underscores longstanding OMB policy concerning sharing government information and interconnecting systems: federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls.

At DHS, the key performance measure of annually reviewing contractor operations showed a minor decrease from 73 percent in 2003 to 67 percent in 2004. Twenty of the Department's contractor operations were not reviewed. The governmentwide performance measure was reported as 83 percent of all contractor operations reviewed. If agencies do not review contractor operations, they cannot be assured that federal data is being handled in accordance with agency requirements.

Security Awareness Training

FISMA requires agencies to provide security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities, and the agency's responsibilities in complying with policies and procedures designed to reduce these risks. Our studies of best practices at leading

organizations¹⁰ have shown that such organizations took steps to ensure that personnel involved in various aspects of their information security programs had the skills and knowledge they needed. Agencies reported that they provided security awareness training to the majority of their employees and contractors. As performance measures for FISMA training requirements, OMB has the agencies report the number of employees and contractors who received IT security training during fiscal year 2004.

DHS reported a substantial increase in the percentage of employees and contractors who received security awareness training in fiscal year 2004. The Department reported that it had trained 85 percent of its staff compared to 14 percent in 2003. As a result, reported performance is comparable to the majority of agencies in this performance measure, as seventeen agencies reported that they had trained more than 90 percent of their employees and contractors in basic security awareness.

Specialized Security Training

Under FISMA, agencies are required to provide training in information security to personnel with significant security responsibilities. As previously noted, our study of best practices at leading organizations has shown that such organizations recognized that staff expertise needed to be updated frequently to keep security employees updated on changes in threats, vulnerabilities, software, security techniques, and security monitoring tools. OMB directs agencies to report on the percentage of their employees with significant security responsibilities who received specialized training.

DHS presented substantial improvement in this performance measure, reporting that it had provided specialized training to more than 90 percent of its employees who have significant security responsibilities. Not only was this a significant improvement over the 66 percent reported in 2003, it also places DHS among the top ten agencies governmentwide for this performance measure. Given the rapidly changing threats in information security, agencies need to keep their IT security employees up-to-date on changes in technology. Otherwise, agencies may face increased risk of security breaches.

Testing of Contingency Plans

Contingency plans provide specific instructions for restoring critical systems, including such elements as arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed due to unexpected events such as temporary power failure, accidental loss of files, or a major disaster. It is important that these plans be clearly documented, communicated to potentially affected staff, and updated to reflect current operations.

The testing of contingency plans is essential to determining whether plans will function as intended in an emergency situation. The frequency of plan testing will vary depending on the criticality of the entity's operations. The most useful tests involve simulating a disaster situation to test overall service continuity. Such a test would include testing whether the alternative data processing site will function as intended and whether critical computer data and programs recovered from off-site storage are accessible and current. In executing the plan, managers will be able to identify weaknesses and make changes accordingly. Moreover, tests will assess how well employees have been trained to carry out their roles and responsibilities in a disaster situation. To show the status of implementing this requirement, OMB requires that agencies report the number of systems that have a contingency plan and the number that have contingency plans that have been tested.

DHS reported a modest increase in the percentage of contingency plans tested. The department stated that it had tested contingency plans for 21 percent of its systems, an 8 percentage point increase over 2003. Moreover, analysis of the numbers reveals that DHS tested 82 plans, which was almost double what it tested in 2003. However, the majority of its systems do not have tested contingency plans. Overall, federal agencies reported that 57 percent of systems had contingency plans that had been tested. Without testing, agencies can have limited assurance that they will be able to recover mission-critical applications, business processes, and information in the event of an unexpected interruption.

Other Challenges in Implementing Statutory Requirements

In addition to the performance measures, there are other requirements that agencies must meet under FISMA. Agencies are required to have a complete and accurate inventory of their major systems and any interdependencies. They are also re-

¹⁰ GAO, *Executive Guide: Information Security Management: Learning From Leading Organizations*, GAO/AIMD-98-68 (May, 1998).

quired to have a remediation process for correcting identified information security weaknesses.

The total number of agency systems is a key element in OMB's performance measures, in that agency progress is indicated by the percentage of total systems that meet specific information security requirements. Thus, inaccurate or incomplete data on the total number of agency systems affects the percentage of systems shown as meeting the requirements. Further, a complete inventory of major information systems is a key element of managing the agency's IT resources, including the security of those resources.

DHS reported that it did not have a complete and accurate inventory in either 2003 or 2004. Without reliable information on DHS's inventories, the Department, the administration, and Congress cannot be fully assured of DHS's progress in implementing FISMA.

FISMA requires each agency to develop a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures and practices of the agency. OMB's implementing guidance refers to this process as a security plan of action and milestones. The chief information officer (CIO) is to manage the process for the agencies and program officials are required to regularly update the CIO on their progress in implementing remedial actions. This process allows both the CIO and the IG to monitor agency-wide progress, identify problems, and provide accurate reporting. In its annual reporting guidance, OMB asks the agency IGs to report on the status of the plan of action and milestones at their agencies. IGs were asked to evaluate the process based on the following criteria:

- known IT security weaknesses from all components are incorporated;
- program officials develop, implement and manage plans for the systems they own and operate that have an IT security weakness;
- program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress;
- CIO develops, implements and manages plans for the systems they own and operate that have an IT security weakness;
- CIO centrally tracks, maintains, and reviews all plan activities on at least a quarterly basis;
- The plan is the authoritative agency tool for agency and IG management to identify and monitor agency actions for corrected information security weaknesses;
- System-level plans are tied directly to the system budget request through the IT business case as required in OMB budget guidance;
- IG has access to the plans as requested;
- IG findings are incorporated into the process; and
- the process prioritizes IT security weaknesses to help significant weaknesses are addressed in a timely manner and receive appropriate resources.

In its 2004 FISMA report, the DHS IG described problems with the plan of action and milestones process at DHS. According to the IG, seven of the nine major department components reviewed lacked a documented and implemented plan of action and milestones. Further, the IG stated that the CIO did not receive reports of remediation progress and did not ensure that components updated the status of their progress. Linkage of the plans to budget requests was reported as minimal at the component level. Seven of the nine components reviewed did not have a formal process to prioritize their IT security weaknesses. Finally, the IG reported that its findings were not incorporated into the plan of action and milestones at DHS. Without an effective, implemented remediation process, DHS cannot be assured that identified security weaknesses are tracked and corrected.

In summary, DHS generally showed increases in the OMB performance measures for FISMA implementation in fiscal year 2004. However, it still faces challenges in implementing the statutory requirements. It faces significant challenges in both inventory development and the implementation of its remediation process. Accordingly, if information security is to continue to improve, agency management must remain committed to these efforts. The annual reports and performance measures will continue to be key tools for holding DHS accountable and providing a barometer of the overall status of its information security.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions from you or members of the Committee.

Should you have any questions about this testimony, please contact me at (202) 512-3317 or Suzanne Lightman, Assistant Director, at (202) 512-8146 or by e-mail at wilshuseng@gao.gov and lightmans@gao.gov, respectively.

Other individuals making key contributions to this testimony include Larry Crosland, Season Dietrich, Nancy Glover, Carol Langelier, and Stephanie Lee.

Mr. ROGERS. Thank you very much.

I just have a couple of questions. I would like to first start with you and then go with Mr. Cooper.

And we would advise you, we may be called for votes at any minute. And we will try to find a good break time to do that.

In listening to your testimony, you talked about how the grade that we referenced in our opening remarks may not be an accurate measure. What do you see as the greatest deficiency or problem with DHS and its information security right now, based on your review?

Mr. WILSHUSEN. Well, based on our review of the FISMA report—

Mr. ROGERS. Right.

Mr. WILSHUSEN. —one of the key elements is, of course, having a complete and accurate inventory, because that is your bottom base-line in terms of being able to track any progress in the performance of securing those systems. If you do not know what the total population of your systems are, it is very difficult to assure that your systems are going to be adequately secure.

Mr. ROGERS. So the inadequate inventory, in your view, is the most glaring problem?

Mr. WILSHUSEN. And the incomplete inventory. That is a key problem. Another key problem, which is that the IG has raised in his testimony—actually, it was the assistant inspector general for information technology at DHS—last week is just the organizational alignment of the CIO and CISO at the departmental level, along with their counterparts at the organizational elements.

Mr. ROGERS. Mr. Cooper, what do you see as the greatest shortcoming in your department and what poses the greatest risk to us as a nation?

Mr. COOPER. I would first confer with what Greg said. And we do recognize that an incomplete inventory is a challenge. The inventory represents—and what I would like to try to do in my answer is tie it into the context of the FISMA scorecard, and help very quickly with a little bit of how the scoring actually impacts the grade and may not fully represent the progress we have made.

The inventory represents basically a negative 10 points. We received no score at all, and still our inventory is certified as greater than 95 percent complete. We currently stand somewhere between 85 and 90 percent complete. That inventory is identified over 3,600 significant applications.

If we compare the quantity with the Department of Transportation, just as an example that was used in a more recent hearing, the Department of Transportation has 480 significant applications. The complexity and the quantity were temporarily against us.

We are on track to complete our inventory some time the early part of Fiscal Year 2006, at which point we will then have a full inventory. Our accreditation of that inventory will, in fact, move from about the current 70 percent probably to about 90 or 95 percent in the same timeframe, so that we will get both the actual work done, and the scoring will be reflected in the FISMA scorecard. That is area number one.

Area number two is in the certification and accreditation of all the applications themselves, and the systems, and the networks,

and all the various moving parts and pieces. We currently stand at about 70 percent. And 70 percent is a failing grade.

Last time I was in school, I could not talk teachers into giving me anything greater than about a D-if I ended up with a 70. That is still true; we recognize it. And we absolutely encourage the committee to hold us accountable to those criteria. We will achieve the desired accreditation and certification. However, it is again not going to occur until Fiscal Year 2006.

The third area is what is labeled in the scorecard "Configuration Management." Now, what that really means is, that for all of the operating systems and the technical platforms that we operate across the department, FISMA requires us to have both policy and guidelines for securing those types of environments and to implement those published guidelines.

Because of our infrastructure transformation initiative, which is a major initiative in the department, I, as the CIO, made a decision—I am the one that you should hold accountable—that we would not actually move to execute or implement some of the configuration management guidelines for those platforms or operating systems that we are going to retire through the conduct of our infrastructure transformation program.

That configuration and implementation of the configuration management, policies and guidelines represents 20 points in the scoring. If you take the inventory minus 10, the configuration management minus 20, we are at 70 before we have done anything else.

Unfortunately, I am here to tell you that in Fiscal Year 2005, we are most likely going to receive an F again. But in 2006, as we complete the program, action and milestones that has now moved from 300 line items in 2004—that was the POAM, that Greg referred to. It now contains over 3,000 line items, action items, that we are actually going to produce and conduct.

But our grade in 2005, most likely, will be an F. In 2006, it will probably move to a B. And it will be that quick. It is going to show up as an F; it will be a B in 2006.

Mr. ROGERS. My time has expired. I thank the gentleman.

And I now recognize the Ranking Member, my colleague from Florida, Mr. Meek, for any questions he may have.

Mr. MEEK. Thank you, Mr. Chairman.

I guess a question for either one of you.

Mr. Cooper, once again, I know that you are in the sunset of your time at the Department of Homeland Security. But I wanted to say how confusing a lot of this is for many of us. A lot of us are well-intended on both sides of the aisle. We understand this issue, because this is where we really come together, as it relates to protecting the homeland.

And we ask the private sector disclosure, you know, when things happen, reporting. I know that is a part of the GAO report about reporting. And when we continue to receive, you know, an F or a D, who are we to criticize the private sector?

The difference between us and the private sector is the fact the nine times out of ten, it is dealing with financial documents, personal information of Americans. But when it comes down to us, it is dealing with, you know, the issue of protecting the homeland, and in some instances, some of our friends and neighbors.

I know that you are leaving. I know philosophy change. So I want you to talk a little bit about how we are going to stay on track and how we are going to improve ourselves, because to the everyday American, I mean, they do not understand half of some of the things that may go on up here. And I will tell you, some of us in the process do not understand half of what is going on up here. And I am serious about that, especially when it comes down to IT issues, that are very important issues.

I know that you talked about integrating a number of systems and also pulling a department together. We are all neophytes as it relates to homeland security, even on this committee, because many of us on this committee, we served in the last select committee and now we have a permanent committee.

But we have departments like Department of Agriculture, which, you know, they do not have the same situation the Department of Homeland Security has had, as it relates to being created in a new agency. Department of Health and Human Services, these are double-F agencies. Department of Energy, I mean, there has not been overhaul of the department to where that they had to find new accountability, nor Housing and Urban Development.

So I am trying to—and if maybe you could address a little bit about what we are talking—given the benefit of the doubt of a new department, and the fact that, you know, we can look forward to an F next year—not look forward to it gleefully, but you are warning us.

And it goes with what the Secretary shared with me yesterday when we were in full committee. And I asked him this question. He said it will be a while before we can get our cards in order, but we need to do it more sooner than later.

Talk a little bit about how this thing is going to live beyond you personally. Who is going to be in place? What kind of attrition are we facing now, as it relates to the individuals that serve under you directly, so that, when we are here a year from now, unfortunately having the same subcommittee hearing? Because we are going to move a bill, from what I understand. There are some members—and I know we have a member of the subcommittee—here today.

Just elaborate on what I have—.

Mr. COOPER. First, sitting behind me is Robert West, who is our chief information security officer in the Department of Homeland Security. Bob is a career federal civil servant with more than 20 years of federal experience in this specific space, in information insurance and information security. Bob's staying. He is not going anywhere.

Most important, though, how are we moving this forward beyond the work that Bob has guided, that I have supported, that the department has supported? The information security systems environment that Bob established has an information system security advisory board.

There are information system security managers from every part of the organizational elements of the department. They are federal people. They maintain the continuity.

The DHS CIO Council that I established contains the CIOs of all of the organizational elements. They are federal career people. They sustain the continuity.

We have put in place an automated tool called Trusted Agent FISMA, which now records—it is actually linked directly into our applications systems environment—and it records all of these progress, the accreditation, the work that is been done electronically so that it becomes a management tool, so that the Secretary, the Deputy Secretary and all of the line managers of the department, not just the IT community, for the first time have visibility into their accreditation status, their configuring management status, their plan of action and milestones. This is all available electronically.

And there is a real-time green, yellow, red indicator, based upon not only the FISMA calibration but also the additional criteria that we have established in the department. At any point in time now—this is now operational. This is real. It is in place. I am not selling you something that we are going to do. It is done.

This enables every key executive in the department to understand exactly where their area of responsibility is, with regard to information security and assurance, and they understand that it is a shared responsibility between the CIO community and the business community to continue to build upon the progress that we have made.

That is one major—second is that, as we complete our inventory, okay, we actually are consolidating. So the environment is becoming less complex. As we consolidate, we have fewer things to accredit. We get better as we go along.

Mr. MEEK. Thank you, Mr. Cooper. I am out of time. We have other members here, and the bell is going to ring soon. But hopefully we will have a second round.

Thank you.

Mr. ROGERS. The gentleman's time has expired.

My colleague from Washington, Mr. Reichert, is recognized for 5 minutes.

Mr. REICHERT. Well, I think it is on.

Mr. ROGERS. It is.

Mr. REICHERT. Thank you, Mr. Chairman.

Welcome. My background is in law enforcement. And one of the major concerns, of course, when you talk about securing information is sharing information. How do you balance the two?

Where in Seattle, in the King County northwest region—and maybe you have addressed this in your initial comments—we have been designated as one of five regions in the country as a test site for the LINX system. The FBI initially chose not to participate. Now they have come to the table and are willing to discuss. Their concern was protecting and securing the information, of course, that they gather and that they have in their files.

We have also, in the northwest region, been selected as one of the four cities in the integration initiative for DHS, along with Cincinnati, Anaheim and Memphis. So there is this effort to integrate information and share information. And I see a conflict there in securing the information but also at the same time in working with local agencies and being able to share that information.

How do you balance those two huge responsibilities?

Mr. COOPER. What we have actually done is we have taken a risk-based prioritized approach. And out of this 3,600 applicants, as

I was saying, what we have actually done is, we have picked the ones that are most important to the mission of homeland security.

For example, those that you described are part of our homeland security information network. That was one of the first applications that we ensured was accredited, certified and had its interim authorities operate. So anything that is moving information from within the department and within the federal environment out into the state and local environment, we have actually focused on those in the early stages.

And all of those applications networks are accredited. They have all of the tools and cybersecurity protection software that we have in place. We monitor those applications and the networks on a 24 by 7 basis. The monitoring is linked into the federal search for the reporting of any incidence or anything that looks suspicious, even suspicious activity, which we can monitor and track.

We believe that this enables the department to ensure that any information going to law enforcement, sensitive and unclassified, and our classified environment, which actually is also thoroughly certified, tested, proved. Our partnerships with the National Security Agency and the intelligence community are all absolutely where they need to be.

Our business systems, on the other hand, we do not have full accredited. Just to give you a quick example and to give you a very, very—response.

Mr. REICHERT. Okay. Do you see the arrival of wireless as complicating your efforts in security, so that officers on the street have real-time information?

Mr. COOPER. It is a challenge, but we have already begun to put wireless-based systems in place using, you know, personal visual assistants, like a BlackBerry, that type of thing, move protected, encrypted information out to Border Patrol agents or out to local law enforcement.

We have operational projects in place that are fully protected, fully accredited. We will continue to do that, again, on this prioritized risk-based approach.

But it does add additional challenges. One that we are struggling with, we actually are trying to figure out the best way to protect the home use of home computers connecting into, for example, e-mail of DHS employees. And as you know, many people have home wireless networks where your neighbor, if you have not properly encrypted it, can enter your own network without you realizing it.

Mr. REICHERT. Right.

Mr. COOPER. So that is a challenge.

Mr. REICHERT. Well, I would just make one last comment, as far as wireless goes. I think, from a local perspective, and working with federal agencies, and making sure that we share information real-time, the wireless technology is critical in that effort. And I certainly recognize the difficult in providing security when you move on to that new technology.

Thank you very much. I yield my time.

Mr. ROGERS. The gentleman yields back.

The gentlelady from Texas, Ms. Jackson-Lee, is recognized for any questions she may have for 5 minutes.

Ms. JACKSON-LEE. I thank the Chairman.

This might be one of the more important subcommittees of the Department of Homeland Security and, of course, responsibilities of the Congress. I said something in the hearing yesterday with the Secretary.

And before I make the same comment very quickly, I just want to acknowledge your work, Mr. Cooper, and of course, Mr. Wilshusen, your work, as well, and all of the employees of the Department of Homeland Security pushed together in a very trying time in America's history and rising to the occasion.

But allow me to ask you to reflect, because I made this statement, that maybe Congress may have made a mistake in its rush to do the right thing. And I say that, and I would appreciate your comment, on the largeness of a 180,000 person-department, which might warrant this committee or the whole committee reviewing if all the pieces that are there now really need to be.

While you reflect on that, would you take note of the fact that the entity that EMS professionals respond to is in DOT. Fire and police are in DHS. And EMS, which are the very principals who deal with a nuclear attack, a chemical attack, with triages on the street, they are in DOT.

And the last point, simply, legislation that we are supporting that goes really to this issue on this whole question of data security or security would put in place an Assistant Secretary of Cybersecurity. Would that be a helpful structure because of ChoicePoint and LexisNexis?

But you would, Mr. Cooper, share your thoughts on the re-imagining, if you will, of DHS, which may add to better security?

Mr. COOPER. Okay. Although I am a certified emergency medical technician and have ridden ambulances in my earlier career, I have to admit that I am not sure that I would be the best person to really comment on the organization of the federal enterprise. I kind of have to defer to Congress, have to defer to those who have had many more years of experience than I in the federal environment.

What I would offer is that I absolutely would encourage this committee, the full committee, and Congress to hold the department accountable for all of the aspects of FISMA and for those challenges around cybersecurity for the nation. That includes the role that the chief information officer plays, the chief information security officer, and our national cybersecurity division, which really is the component that looks externally for the department.

I, as the CIO, have the internal responsibility for complying with FISMA and ensuring that all of the information technology assets of the department are secure, including the data aspects of that.

I would also suggest that we are absolutely on the right track in the information-sharing initiative, which is federal, enterprise-wide initiative, as you know, under the Executive Order 13336, although do not hold me fully to the proper number. I will relay that back to the committee, if necessary.

Under the guidance of the Office of Management and Budget, significant work architecturally is being done that I think will ensure that, regardless of the organizational structure, the right information, regardless of its source in whatever federal department exists, can, in fact, be exchanged with other parts of the federal enterprise and appropriate authorities in state and local, tribal gov-

ernments, and the private sector that has responsibility for critical infrastructure.

Ms. JACKSON-LEE. Can I ask that Mr. Wilshusen, if he would comment on the largeness and the possible need of reviewing all of the elements of the DHS, which deals with security—what might help it contain its security issues?

Mr. WILSHUSEN. I would also just like to comment on what Mr. Cooper just mentioned, too, and kind of expand on that, in terms of what the Congress' responsibility to help provide oversight in holding the agency officials accountable.

FISMA also gives specific responsibilities to the agency head. It is not just the CIO's responsibility or the chief information security officer's responsibility. Overall responsibility rests with the agency head. So certainly, keeping the agency head and other senior program officials, who also have specific responsibilities under FISMA, also need to be held accountable and made aware of their responsibility.

Ms. JACKSON-LEE. Thank you.

Mr. ROGERS. The gentlelady yields back.

The chair now recognizes the Chairman of the full committee, Mr. Cox from California.

Mr. COX. Thank you very much.

And I want to thank our witnesses for being here. I know that you both have been working on this issue for some time, Mr. Cooper in particular, specifically in the Department of Homeland Security.

I want to make sure I understand the evaluation that we have been given. Agency inspectors general were asked several questions to evaluate and verify whether various departments in the government, and specifically the Department of Homeland Security, maintain and update an effective plan of action. They were asked whether the Department of Homeland Security maintains and updates milestones in order to remediate security weaknesses.

So my understanding is that the responses to those questions go not to whether or not we have secure systems in place at DHS, but rather whether the process—an easier test—whether the process that is in place to get us there is a good one.

And that even in response to that easier question, if it is the process that is designed to get us secure a good one, the answer came back, essentially, no. But I want to make sure that my understanding is correct.

There is a column—and, Mr. Wilshusen, I am going to direct this to you, because I think that this is your line of inquiry. All of the agencies, from AID to Veterans Affairs, are listed. DHS is one of those agencies. And the questions about an effective plan of action and milestones were put. There was a column that says, "Verified: Yes, No." And the answer for the Department of Homeland Security is "no."

Does that mean that you just did not verify it or that you could not verify it because there was a problem?

Mr. WILSHUSEN. FISMA requires each agency and their inspector general to report on the progress of the agency in implementing the provisions of FISMA. OMB and one of its responsibilities is giving reporting instructions to the agencies and IGs and how—in both

the form and content of how to report those—to meet that reporting requirement.

OMB requires two types of information. One, they do require performance measures in reporting how agencies have implemented different information security requirements, for example, the percentage of systems that have been certified and accredited.

In addition, OMB has asked the inspector generals, or inspectors general, to review the quality of some of the processes at those agencies, such as the process for certifying and accrediting their systems as well as the department process for developing a plan of action and milestones.

In specific response to your question, “Is that verified?” is that the IG for that particular issue has said that they do not have a strong or a good process for that.

Mr. COX. All right, so this is not simply a matter of our not being able to verify the answer to the question. Rather, it goes to the lack of a sound process?

Mr. WILSHUSEN. If that is from the FISMA 2004 report, I believe that is correct.

Mr. COX. That is exactly right. That is what I am quoting.

Mr. WILSHUSEN. Okay.

Mr. COX. And that is what it means.

Mr. Cooper, help me with why we should not be concerned about this?

Mr. COOPER. Last year, you should have absolutely been concerned. So were we. I certainly am not proud of our failing grade. And we take it very seriously.

And what that reflects is exactly correct. Our inspector general, working with us, and kind of looking over our shoulder at the work we have done, labeled our plan of action and milestones process to get us to all of the things that we want to get done as poor. And we agreed.

Here is the good side of the story. Last year, we had about 300 line items, meaning specific tasks that we needed to take. This year, in the ensuing time, our report this year will not only show that we have a very good, robust process, but we now have over 3,000 action items identified. That is the difference between a poor process not well-executed and a good process properly executed.

I am very confident that, although we still will most likely receive an overall failing grade, which again we are not going to be proud of—

Mr. COX. But let me make sure I understand. If the grade is given not on whether your computers systems are secure but rather on whether you are following a process to get them there, why would not you get a passing grade?

Mr. COOPER. It is both. It is both. In other words, the process represents actually only about 15 points of the 100 that comprise the total score. But we only received two points, because of our poor process and nothing in the plan.

The accreditation and certification represents about 20 percent of the total grade. We received zero points, okay? This year, we will receive significantly greater points in each area.

But the total score that also includes things like annual testing, configuration management, incident protection, and response and

reporting, when you total up all those different categories—and there are seven or eight major categories—we still will not aggregate enough points—A, B or higher, we believe. This is what I am projecting, and this is what I am telling you.

We are on track, however, we believe, to achieve a score significantly higher, probably we believe a B, by the end of Fiscal Year 2006. But the reality for the Department of Homeland Security, our environment is large enough, complex enough, and has so many different moving parts and pieces. We are moving as quickly as we can, but we must move with quality and with speed.

And we just do not believe we cannot get there faster than Fiscal Year 2006.

Mr. COX. Mr. Chairman, my time has expired. I do not know if—I did not realize there were votes on the floor. I yield back.

Mr. ROGERS. The gentleman yields back.

I do want to thank both of you again for your statements. And your answers have been very helpful. We have been called for two votes, so we are going to excuse both of you all and ask our second panel, if you could, to be patient with us.

We are going to run over and vote, and we will be right back for the start of our second panel. Thank you very much.

We are in recess, subject to the call of the chair.

[Recess.]

Mr. ROGERS. The chair would like to call this meeting of the subcommittee back to order.

And I thank our panelists for their patience, but we had to go vote. And I would now like to recognize Mr. Mark MacCarthy, senior vice president for public policy at Visa USA to testify.

Your statement?

**STATEMENTS OF MARK MacCARTHY, SENIOR VICE PRESIDENT
FOR PUBLIC POLICY, VISA USA**

Mr. MACCARTHY. Thank you, Mr. Chairman and ranking minority member.

My name is Mark MacCarthy. I am the senior vice president of public policy for Visa USA. I appreciate the opportunity to address the important issues raised by today's hearings on the need to strengthen information security.

The Visa payment system, of which Visa USA is a part, is the largest consumer payment system in the world, with more volume than any other payment system and, indeed, with all other payment systems combined. We play a pivotal role in advancing new payment product and technologies, including technology for protecting personal information and preventing identity theft and fraud.

Visa commends the subcommittee for focusing today on this important issue. As the leading consumer electronic payment system, Visa considers it a top priority to remain a leader in the development of services and technologies that protect information and protect consumers from the consequences of information security breaches.

We have long recognized the importance of strict internal procedures to protect the customer information that is housed within Visa's databases and the databases of our members.

We have a strong incentive to have a good security proceedings in place. The Visa system provides for zero liability for cardholders when unauthorized transactions take place. Cardholders are not responsible for the unauthorized use of their card. This Visa zero-liability policy guarantees the maximum protection for Visa cardholders against fraud.

And because the financial institutions within the Visa system do not hold their cardholders responsible for that unauthorized fraud, Visa institutions incur costs. These costs include the direct costs of fraud, the credit that is not repaid, and can also be in the form of indirect costs attributable to the harm of consumers and to merchants generally. Accordingly, Visa protects the customer information of its members vigorously.

We are currently implementing a comprehensive and aggressive consumer information security program. It is called a cardholder information security program. Its acronym is CISP. This security program applies to all entities, including merchants that store, process, transmit or hold Visa cardholder data and covers enterprises that operate through brick-and-mortar operations, mail and telephone order operations, or through the Internet.

CISP was developed to ensure that the customer information that Visa's members have got is kept protected and secure. CISP includes not only data security standards but also provisions for monitoring compliance and sanctions for failure to comply.

As part of CISP, Visa requires all participating entities to comply with our Visa "Digital Dozen," 12 basic security requirements for safeguarding accounts. These include to install and maintain a working firewall to protect data.

Do not use vendor supplies defaults for system passwords and security parameters. Protect stored data. Encrypt data sent across public networks. Use and regularly update anti-virus software. Develop and maintain secure systems and applications.

Restrict access to data on a need-to-know basis. Assign a unique I.D. to each person with computer access. Restrict physical access to data. Track all access to network resources and data. Regularly test security programs and processes. And implement and maintain an overall security program.

For the largest companies, for those companies that process more than 6 million Visa transactions per year, we require an annual on-site audit, validated by an independent security assessor, or in the alternative, an internal audit signed off by an officer of the company.

We also require quarterly network scans validated by a qualified, independent scan vendor. Visa provides lists of recommended security assessors, scan vendors, and software providers for the use of merchants and others who have the need for that service.

Visa takes enforcement action against companies that do not implement adequate security. Visa members are subject to fines of up to \$500,000 per incident for any merchant or service provider that is comprised and is not compliant with our CISP program at the time of the incident.

Visa is not the only organization that has developed security standards. In order to avoid the potential for conflicting requirements on merchants and others, in December of 2004, Visa,

MasterCard, American Express, Discover, and Diner's Club collaborated to align our data security requirements for merchants and third parties.

We found that the differences between these security programs were largely procedural, not substantive, and we had—therefore we were able to integrate our CISP program into a common set of data security requirements without diluting the substantive measures that were already in place for information security.

This new common set of data security standards is called the PCI standard. It invokes a common framework for four fundamental aspects of information security.

First, it details technical requirements for the secure storage, processing and transmission of cardholder data. It contains common security auditing procedures. It enables participants to cross-recognize their respective certification programs for vendors. And fourth, it allows for the restructuring of the program so that each has similar merchant and service-provider validation requirements.

This new alignment allows merchants and service providers to select one vendor and implement a single process to comply with all of the payment card requirements. Instead of fragmenting their resources to satisfy separate requirements, this standard allows merchants and service providers to focus on achieving a common objective, namely the robust and continuously updated security programs that we all want.

In addition to the CISP program, Visa uses sophisticated neural networks that flag unusual spending patterns for fraud. And you block the authorization of transaction where fraud is suspected.

When cardholder information is compromised, Visa notifies the issuing financial institution. We put the affected card numbers on a special monitoring status. And if Visa detects any unusual activity in that group of cards, we again notify the issuing institutions who begin a process of investigation and card re-issuance.

Mr. Chairman, I have some additional information about programs that Visa has in place for identity theft. And I respectfully request that that information be made part of the record of this hearing.

Mr. ROGERS. Without objection, it is.

Mr. MACCARTHY. Thank you for this opportunity to testify, and I am prepared to answer any questions you may have.

[The statement of Mr. MacCarthy follows:]

PREPARED STATEMENT OF MARK MACCARTHY, SENIOR VICE PRESIDENT, PUBLIC POLICY, VISA USA

Mr. Chairman, my name is Mark MacCarthy. I am Senior Vice President for Public Policy for Visa U.S.A. Inc. Visa appreciates the opportunity to address the important issues raised by today's hearing on the need to strengthen information security.

The Visa Payment System, of which Visa U.S.A. is a part, is the largest consumer payment system, and the leading consumer e-commerce payment system, in the world, with more volume than all other major payment cards combined. Visa plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information and preventing identity theft and other fraud.

Visa commends the Subcommittee for focusing on the important issue of information security. As the leading consumer electronic commerce payment system in the world, Visa considers it a top priority to remain a leader in the development of technology, products, and services that protect consumers from the effects of information security breaches. As a result, Visa has long recognized the importance of strict in-

ternal procedures to protect the customer information of Visa's members, thereby protecting the integrity of the Visa system.

Visa has substantial incentives to maintain strong security measures to protect customer information and the Visa system overall. The Visa system provides for zero liability to cardholders for unauthorized customer transactions. Cardholders are not responsible for unauthorized use of their cards. The Visa Zero Liability policy guarantees maximum protection for Visa cardholders against fraud due to information security breaches. Because the financial institutions that are Visa members do not impose the losses for fraudulent transactions on their cardholder customers, these institutions incur costs from fraudulent transactions. These costs are in the form of direct dollar losses from credit that will not be repaid, and also can be in the form of indirect costs attributable to the harm and inconvenience that might be felt by customers or merchants. Accordingly, Visa aggressively protects the customer information of its members.

Visa's Cardholder Information Security Plan

Visa is currently implementing a comprehensive and aggressive customer information security program known as the Cardholder Information Security Plan ("CISP"). This security program applies to all entities, including merchants, that store, process, transmit, or hold Visa cardholder data, and covers enterprises operating through brick-and-mortar stores, mail and telephone order centers, or the Internet. CISP was developed to ensure that the customer information of Visa's members is kept protected and confidential. CISP includes not only data security standards but also provisions for monitoring compliance with CISP and sanctions for failure to comply.

As a part of CISP, Visa requires all participating entities to comply with the "Visa Digital Dozen"—twelve basic requirements for safeguarding accounts. These include: (1) install and maintain a working network firewall to protect data; (2) do not use vendor-supplied defaults for system passwords and security parameters; (3) protect stored data; (4) encrypt data sent across public networks; (5) use and regularly update anti-virus software; (6) develop and maintain secure systems and applications; (7) restrict access to data on a "need-to-know" basis; (8) assign a unique ID to each person with computer access; (9) restrict physical access to data; (10) track all access to network resources and data; (11) regularly test security systems and processes; and (12) implement and maintain an overall information security policy.

Audits

For the largest companies, those who process more than 6 million Visa transactions per year, we require an annual on-site audit validated by an independent security assessor, or an internal audit signed by an officer of the company. Visa also requires quarterly network scans validated by a qualified independent scan vendor. Visa provides lists of recommended security assessors, scan vendors, and software providers.

Sanctions

Visa takes enforcement action against companies that do not implement adequate security. Visa members are subject to fines, up to \$500,000 per incident, for any merchant or service provider that is compromised and not CISP-compliant at the time of the incident.

Payment Card Industry Data Security Standard

Visa is not the only credit card organization that has developed security standards. In order to avoid the potential for imposing conflicting requirements on merchants and others, in December of 2004, Visa, MasterCard, American Express, Discover, and Diners Club collaborated to align their respective data security requirements for merchants and third parties. We found that the differences between these security programs were more procedural than substantive. Therefore, Visa has been able to integrate CISP into a common set of data security requirements without diluting the substantive measures for information security already developed in CISP. Visa supports this new, common set of data security requirements, which is known as the Payment Card Industry Data Security Standard ("PCI Standard").

The PCI Standard provides a common framework that encompasses four fundamental aspects of information security:

- **Technical Foundation:** The PCI Standard details technical requirements for the secure storage, processing, and transmission of cardholder data.
- **Testing Methodologies:** The PCI Standard promotes the development of common security auditing procedures, scanning procedures, and provides a common security Self-Assessment Questionnaire.
- **Vendor Certification:** The PCI Standard enables participants to cross-recognize their respective certifications for vendors. In particular, MasterCard has

agreed to recognize Visa-approved onsite security assessors, and Visa will recognize MasterCard security scan vendors.

- **Compliance Validation:** The individual security programs maintained by payment card systems, such as Visa's CISP or MasterCard's security program, have been restructured within the framework of the PCI Standard so that each has similar merchant and service provider-levels and validation requirements.

The new alignment of security standards under this framework allows merchants and service providers to select one vendor and implement a single process to comply with all payment card data security programs. Instead of fragmenting their resources to satisfy separate requirements, the PCI Standard allows merchants and service providers to focus on achieving a common objective: robust and continuously upgraded security programs.

Neural Networks to Detect Fraud and Block Potentially Unauthorized Transactions

In addition to the CISP program, Visa uses sophisticated neural networks that flag unusual spending patterns for fraud and block the authorization of transactions where fraud is suspected. When cardholder information is compromised, Visa notifies the issuing financial institution and puts the affected card numbers on a special monitoring status. If Visa detects any unusual activity in that group of cards, we again notify the issuing institutions, who begin a process of investigation and card re-issuance.

Mr. Chairman, Visa has additional information about its programs to prevent identity theft and to aid customers to recover from identity theft. I respectfully request that information relating to these programs, and to the programs which I have described in my testimony, be included in the record of this hearing.

Thank you, again, for the opportunity to present this testimony today. I would be happy to answer any questions.

Mr. ROGERS. Thank you, Mr. MacCarthy, for your testimony.

The chair now recognizes Mr. Mark Zwillinger, partner at Sonnenschein, Nath and Rosenthal, for his opening statement.

MR. MARC J. ZWILLINGER, ISSP NATIONAL CHAIR, INFORMATION SECURITY AND INTERNET ENFORCEMENT GROUP

Mr. ZWILLINGER. Thank you.

Chairman Rogers and Ranking Member Meek, thank you for inviting me to speak with you today on the topic of strengthening information security at DHS. As you know, I am a former computer crime prosecutor from the Department of Justice, and I now run the information security and enforcement practice at Sonnenschein, Nath and Rosenthal.

In my legal practice, I help private-sector clients develop and implement information security programs and effective instant response plans. My clients come from a variety of industries, and they include major financial institutions, Internet service providers, satellite broadcasters, and traditional media publishers.

In addition to my client work, I have participated in two efforts to help secure the nation's critical infrastructure. First, I served on the National Academies' Committee on Critical Infrastructure Protection and the Law, and most recently, I served on the Corporate Information Security Working Group, which provided advice to the House Committee on Government Reform.

But I sit before you today not on behalf of my clients but to use my information security experience from the private sector to try to be helpful on the topic of strengthening DHS' information security programs. With that goal, I would like to share some lessons that I have learned from my experience in the private sector.

First, we all understand that government computer systems are attractive targets for a variety of reasons, the critical nature of the information stored on the systems, the potential for serious disrupt-

tion of government operations, and the continued inadequacy of security controls at many agencies. Of course, only the last of these factors is completely within the government's control, and FISMA was supposed to bring improvement in this area.

As you know, FISMA requires each federal agency to provide information security protections that are appropriate to the risk of harm that might result when a system is compromised. This same risk-based approach is found in almost all information security legislation and in all best-practices guides in the private sector.

However, I have seen in the private sector that, no matter how valuable the information is that is contained on computer systems, a standard risk analysis is generally not sufficient to motivate true organizational commitment to security. Instead, such commitment is spurred by ancillary factors, such as the damage to the company's public reputation and possible financial harm that could result from such damage.

In fact, one of the key reasons why some in the private sector are predisposed against legislation requiring notice in the event of a security breach is that, when the risk of a security breach includes the risk of public disclosure of that breach, the analysis virtually requires an investment in security for several reasons.

First, the public disclosure alone would have the potential to tarnish a company's reputation, interfere with their customer relationships, and drive down their market value. Second, the public disclosure creates an increased potential for litigation, especially now, which threatens direct financial loss, as well as additional publicity.

So if these types of consequences are necessary to change the risk calculus in the private sector, how do we change the risk calculus in the public sector? And it appears that FISMA report cards were designed to do just that. By making FISMA compliance public in a very simple-to-understand way, the goal was to use the negative stigma of receiving an F grade to bring about more positive results.

However, without the marketplace effect, the risk of getting an F in the public sector is not nearly as threatening, and not, therefore, as motivational as a similar failure in the private sector, even though the consequence of a compromise at DHS could be a lot worse.

One fix would be to seek to incentivize behavior in the same way as in the private sector. This might translate into responding to poor information security performance with stronger oversight or more exacting audits. It may also include tying security performance to the private sector equivalent of profit, mainly funding.

A second lesson is that many of the security breaches I have seen recently have involved compromises of data given to third parties without a clear allocation of responsibility for security and for notification. On the whole, both the public and private sectors tend to worry far less about their data when it is given to others to manage, when the exact opposite should be true.

Third, the importance of a proper incident-response program cannot be overstated. No set of policies, procedures, or practices can achieve a goal of making an agency completely secure. But my experience with the private sector suggests that organizations that

aspire to have a robust incident-response program not only discover and address event before they become serious, but by following their plan and fixing the detected vulnerabilities, they can significantly improve their overall security posture.

DHS' performance on the FISMA categories of tested contingency plans and effective security and privacy controls suggest that either the department's incident-response plan is lacking or its execution requires some improvement.

Finally, Mr. Chairman, having read the testimony of DHS officials and listening to Mr. Cooper today, I think you would be hard pressed to find many security experts who would say that DHS is saying the wrong thing.

Instituting a strategic plan, working to institute DHS policies throughout all of its organizational components, completing its inventory, and collecting and verifying metrics are steps in the right direction. Nevertheless, creating a true culture of security certainly remains an evolving challenge at DHS.

My clients, who have been most successful in creating a culture of security, are easy to distinguish from those who have not. While most organizations have talented people attending to information security, the priorities have to be set from the top down and carried throughout the organization.

For example, one of my clients, in addition to all of the information security policies and procedures they have, they bring in all of their product engineers from around the world for an annual multi-day conference on security issues, despite the time spent away from revenue-producing work.

In my view, this conference is but one example of how that company gets it. For them, information security is not all about return on investment or liability prevention. It is an essential part of their product development lifecycle and their culture.

For the sake of the country, I would hope that the same could be said about DHS in the very near future.

Mr. Chairman, thank you for your leadership in convening this important hearing. I hope I can provide further help by answering your questions now or in the future.

[The statement of Mr. Zwillinger follows:]

PREPARED STATEMENT OF MARJ J. ZWILLINGER, PARTNER, SONNENSCHN NATH & ROSENTHAL LLP

Chairman Rogers, Ranking Member Meek, and Members of the Subcommittee, thank you for the opportunity to address the Subcommittee on the important topic of Strengthening Information Security at the Department of Homeland Security

Background

I have been a lawyer in the field of Information Security since 1997 when I was a Trial Attorney at the United States Department of Justice Computer Crime and Intellectual Property Section.

Since 2000, I have been leading an Information Security Legal practice at a national law firm. In my daily practice at Sonnenschein Nath & Rosenthal, I help private sector companies develop and maintain effective information security programs and incident response plans. While this may not be traditional legal work, I am not a traditional lawyer, as I am also a Certified Information Systems Security Professional and have training in computer forensics and network investigations.

In addition to my work with private companies, I have been part of two efforts to provide ideas to help secure the nation's critical infrastructure. First, I served as a member of the National Academies' Committee on Critical Information Infrastructure Protection and the Law. Second, I had the privilege of being invited to partici-

pate as the sole independent lawyer on the Corporate Information Security Working Group, which advised the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. As with my testimony here today, my participation in both of those efforts was not on behalf of any client, but was an attempt to use my experience of representing clients in the information security space to help our country better protect its information assets.

Ironically enough, both of those prior efforts were geared towards finding better ways to motivate the private sector to protect the portions of the critical infrastructure under its control. However, now that a spate of industry-specific regulation and high-profile breaches of consumer information seem to be motivating the private sector to action, and given the Sarbanes-Oxley environment in which spending money on internal controls is becoming commonplace, it may be the public sector that could most benefit from additional attention.

About the Threats to Government Systems

When I was a computer crime prosecutor, it was conventional wisdom among hackers that government agencies and educational institutions were the low-hanging fruit of the computer world. These entities presented attractive targets because of the bandwidth and power of the computer systems available, and because the security at both types of institutions was ineffective.

When the focus of computer crime shifted away from the availability of computer resources to the market value of information stored on computer systems, the private sector became an interesting, and potentially lucrative, target.

But while that shift may have diminished the interest in hacking university systems (except as we have recently learned for the purpose of identity theft), government systems remain an attractive target for several reasons:

- (1) the power and bandwidth of these computer systems;
- (2) the critical nature of the information stored on such systems;
- (3) the potential for significant disruption of critical government activities; and
- (4) the inadequacy of security controls at many government agencies.

Of these factors, only the fourth is completely within the government's control. And the Federal Information Security Management Act (FISMA) was designed to change the way government agencies addressed this fourth factor. FISMA requires the head of each federal agency to provide information security protections that are commensurate with the risk and magnitude of harm that might result from unauthorized access, use, disclosure, modification or destruction of the information contained on such systems.

Changing the Risk Calculation

The same risk-based approach is contained in almost all information security legislation, regulations, and best practice guides that are used by the private sector, and always includes an assessment of the value of the information stored on the computer systems. What I have seen when counseling my private sector clients on information security issues, however, is that the motivation to improve information security relates not just to the value of the information at issue, but to several ancillary factors. In fact, private sector information may be less sensitive and present a lower risk of harm to the nation's security if compromised, but it is at times better protected than DHS information.

The risk that is evaluated and, with increasing frequency, acted upon by private corporations is the damage to the corporation's public reputation and the financial harm that may result. In fact, one of the key reasons that the private sector is sometimes predisposed against security breach notification legislation, such as the bills already introduced in the 109th Congress, is that when the risk of compromise of a system becomes the risk of public disclosure of that compromise, the consequences virtually demand a significant investment in security by every right-minded CEO or CIO of a public company for several reasons.

First, the public disclosure itself has the potential to drive down market value of a corporation. Second, disclosure of such breaches, irrespective of resulting harm, tarnishes the corporation's reputation and interferes with customer relationships. Third, the public disclosure of breaches also creates an increased potential of litigation, threatening direct monetary loss as well as additional adverse publicity and lower market value.

As a result, these potential consequences are powerful enough to drive a corporation to invest in security even where the information stored is not as valuable as DHS data, because any breach directly threatens corporate financial results.

Lessons Learned

First, as I have described, risk assessments that focus solely on the value of the information to be protected have often been unsuccessful on their own in motivating

good information security behavior. Accordingly, external forces caused a change in the risk calculus. But how do you change the risk calculus for the public sector?

FISMA report cards were designed to accomplish that objective. By identifying the agencies that were not meeting FISMA standards in a more public way than the detailed descriptions contained in the OMB reports, the associated stigma was intended to raise the profile of non-compliance, thereby creating incentive for action. However, absent a market value determination, the risk associated with receiving a failing grade is not nearly as catastrophic, nor as motivational, as it is in the private sector, even though the consequences of a compromise of DHS information may be greater.

Accordingly, FISMA compliance, and public sector information security in general, could be bolstered by offering incentives based on what we have seen work in the private sector. This includes responding to poor information security performance with stronger oversight or more exacting audits, and rewarding good security practices with positive incentives. It may also include tying security performance to the private sector equivalent of profit, namely funding. While it may seem offensive to suggest that the threat of a loss of our nation's most sensitive and critical information is alone an insufficient incentive to improve information security, DHS's FISMA performance to date suggests that additional action may be warranted.

The second lesson is that many, if not most, of the breaches to which I have responded in the past four years have included compromises of data that was placed in the hands of third parties without a clear allocation of responsibility for security issues, or procedures for notification and response in the event of a breach. Given that of all the issues identified in OMB's 2004 FISMA report, DHS fared the best on "using appropriate methods to ensure that contractor-provided services are adequately secure," perhaps the private sector has something to learn from the government in this regard. On the whole, however, both sectors tend to worry less about data maintained by others, when the exact opposite should be true.

Third, as noted in the National Institute of Standards and Technology (NIST) Incident Handling Guidelines, "an incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computer services." In my experience with the private sector, organizations that have a robust incident response program not only catch incidents before they become serious, but in executing the incident response plan and remediating the vulnerabilities that are detected as a result of the plan, achieve a much improved security posture. DHS' poor performance on the FISMA categories of "tested contingency plans," and "effective security and privacy controls," suggests that either the Department's incident response plan is lacking, or its execution requires improvement.

Finally, Mr. Chairman, your Subcommittee would be hard-pressed to find too many security experts who would say that DHS is saying the wrong things. That is, instituting an Information Security Program Strategic Plan, working to institute DHS-wide policies within the organizational components, and collecting and verifying performance metrics are positive steps in the right direction. Nevertheless, the objective must be to create a culture of security within every organization, which clearly remains an evolving challenge in these early days of DHS.

My clients who have been successful at creating a culture of security can be easily distinguished from those that have not. For example, one of my clients flies in all of its product engineers, located domestically or internationally, for an annual multi-day conference on security issues, despite the time spent away from revenue-producing activities. In my view, that company clearly "gets it." Information security is not all about return on investment or liability prevention, rather, it is an essential component of their product development lifecycle and their culture. For the sake of the country, I would hope the same could be said about DHS in the very near future.

Mr. Chairman, again, thank you for your leadership in convening this important hearing and I stand ready to be of further assistance through answering your questions now or in the days ahead.

Mr. ROGERS. Thank you, Mr. Zwillinger, Zwillinger. What is the correct pronunciation?

Mr. ZWILLINGER. Zwillinger.

Mr. ROGERS. Zwillinger, for your testimony.

I now have a couple of questions. And I would like to start with you.

You were here for the first panel's testimony. And when you think about your clients that you deal with, what is the suggestion that you would offer this committee as a change that we could focus our attention on to remedy the problems that we are seeing reflected in this F grade?

Mr. ZWILLINGER. Well, based on my experience with clients, I find that the organizations in companies that are able to really carry security throughout their organization have a very top-down approach. That is, the CIO or the chief information security officer is empowered throughout the organization to make sure that the organization is complying with security practices and carrying through with its mission.

And I have not studied DHS long enough to know how deep a problem this is within the organization. I do note that when Frank Deffer testified before the House Committee on Government Reform, he pointed to a lack of formal reporting structure between the CIO and its organizational components. I do not know if that is the case or not at DHS, but I know that generally in the private sector that is an important feature, if the CIO can control the policies from the top down.

Mr. ROGERS. You heard reference earlier about the problems with inventory that are described as kind of the biggest challenge that DHS faces. Do you see a similar problem with getting your arms around inventory and applications on the inventory in the private-sector clients that you have, as was presented earlier by the DHS testimony?

Mr. ZWILLINGER. Certainly, the clients I work with do conduct an inventory at the very beginning of a risk assessment, determining their assets and defining which assets are most critical. So I do see that that is a hurdle that most of my clients have to overcome.

I cannot really comment on the length of time that it is taken DHS to conduct that inventory, but I do know that conducting inventory is an important first step and should be completed at the first stages of the security program.

Mr. ROGERS. Thank you.

I would like to ask Mr. MacCarthy, what kind of management organizational structure and line of authority does Visa have in place to address information security issues?

Mr. MACCARTHY. We have a chief information officer who has full authority within Visa to make the decisions that he needs to make in order to ensure that the Visa system itself is safe and secure.

Our program for spreading good security to the institutions outside Visa is under our risk control operation. And they work closely with the member banks within the Visa system, who in turn work closely with the merchants. Visa has every incentive to do the right thing with respect to information security.

One of the things that—Mark's comments on the contrast between the private sector and the public sector deserves some emphasis. Why do we take these steps for information security within the Visa system and with respect to merchants? And the answer is, because fraud losses within our system fall on our members. And anything we can do to prevent the information security breaches means we minimize those fraud losses.

We spend \$300 million a year on information security and fraud control. And those kind of investments pay off. Our fraud rate is now down at the level of 5 cents for every \$100, and it continues to go down year after year because of those investments.

So I think one of the big contrasts between the public sector and the private sector here is the incentives that different companies have for practicing good information security.

Mr. ROGERS. Well, you make a good point in referring to the litigation, the exposure that you would have. But in response to that, I would say, do you have a formal reporting process in place for capturing known security weaknesses?

Mr. MACCARTHY. Absolutely. Within the Visa system itself, it is internal. And you know, we have regular audits of our own systems and any—

Mr. ROGERS. But is this written policy?

Mr. MACCARTHY. Yes, this is. Any deficiencies we catch, you know, we step in and correct right away. Within the Visa system itself, any breaches on the part of our financial institutions who are part of the Visa system, or on merchants, or processors who have cardholder information, they are required by contract to report those breaches to us immediately. And they are fined some other penalties that result for them not reporting those kind of breaches to us instantaneously.

Mr. ROGERS. Do you have outside audits of your security system?

Mr. MACCARTHY. Oh, yes, sir. Oh, yes.

Mr. ROGERS. Conducted by who?

Mr. MACCARTHY. I will get you the answer on that. There is an outsider auditor that we use for that purpose.

Mr. ROGERS. Great. Thank you both.

The Chairman now yields to the Ranking Member, Mr. Meek.

Mr. MEEK. Thank you very much, Mr. Chairman.

Gentlemen, I want to thank you for your testimony. As you can tell, there are a number of members of the Congress that are very concerned about how we are exposed, I feel, to not—I mean, to negative forces that are out there, especially as it relates to homeland security.

And I was—both of you, I was taking a look at your testimony here. And from what I heard, both of you are driven in the private sector. And I am pretty sure that you have taken a look at the GAO report. And to see the position, not only the Department of Homeland Security is in now, and you heard earlier testimony to the fact that it will be Groundhog Day next year, this time, if things are left up to the mechanics of the department and others.

Looking at the position that the department is in, along with four or five other agencies of the federal government, and the federal government overall receiving a D-plus by our own eyes and ears, and looking at the tools that were used, where auditor generals basically ask questions to work with the IT officials within those departments. Pretty much, you are given a test, but you also have the opportunity to use whatever materials that you may find to answer the question.

If there was a private sector company, let us just say, Mr. Z—
[Laughter.]

I was dying to say that. I know people—do people call you Mr. Z?

Mr. ZWILLINGER. All the time.

Mr. MEEK. I know. It is just so cool.

If there is a private-sector company in the position of the Department of Homeland Security, how long will it take that company to bring itself up to some sort of reasonable level that what we would find with using our measuring stick to bring it to a C or a B.

How long would that take? Will that take an experience of 3 or 4 years to improve its footprint, or will it take the time that we are being told that it would take for the department to bring itself up to standard?

Mr. ZWILLINGER. It is a very difficult question for me to answer, one, because my clients are not generally of the size and scope of DHS, nor have they dealt with the integration of the equivalent of 42 subsidiaries, or what number of subsidiaries in a very short period of time.

That being said, I have seen considerable progress in all of the clients that I have worked with in the security space from the time that I left DOJ and started practicing information security in 2000, you know, within a couple of years, if they have decided to invest significantly in security.

So I understand the problems with DHS must be daunting. And I do not know that there is a real private sector analog that I can really draw upon to answer your question.

Mr. MACCARTHY. If I could comment, I think it is important not to overstate the extent to which the private sector is automatically doing the right thing in the area of information security. I think largely the incentives are aligned right, but it is important to remember that, that for many companies, information security is a cost.

You have got to invest in the technology. You have got to invest in the time and training of your personnel. There is some loss of functionality in some cases.

And you are protecting yourself against relatively rare events. And when the bad things do occur, there is a breach, you know, the costs are sometimes distributed. They do not fall just on the company involved, but they fall on other parties. So there is a kind of externality in that, where the market forces do not always automatically align to create, you know, perfect incentives to invest in information security.

That is one reason why Visa stepped in with this CISP program, because we wanted to make sure that, when the fraud losses fall on our member financial institutions, but the security investments has to be made by merchants and others who house the data, that there was some sort of private-sector mechanism involved that could try to internalize that market externality.

We are aware that there are no rules and regulations under federal law or state law that require information security for merchants. And so we stepped into the breach to see what we could do to try to correct that particular difficulty.

Mr. MEEK. I guess, you know, gentlemen, where my concern comes in—as you know, the private sector—and you talk about reporting a little earlier as it relates to embarrassing for that pri-

vate-sector company. We know that computers are hacked everyday. Some people are held up online literally for a price. And it goes unreported.

It is not public knowledge, you know, the top-secret information and posture, and how our IT is so vulnerable in the federal level is not—I mean, it is common knowledge. We have things that you call exercises related to TOPOFF programs, intelligence information that is shared, not only with state and local government, but also with federal agencies within.

Some may argue that there is a higher level of security as it relates to our information technology, the higher security level may go, but there are people who live to get that kind of information as it relates to national security.

And you are right that this is the largest agency in the history of the world, I mean, as we live in it. But at the same time it is important as one of the most—the most able country, in my opinion, for us to be able to move forth. We have to. I mean, the Chairman, myself, the Ranking Member and the overall chair, we are going to be held ultimately responsible for being the Oversight Committee if we do not apply the pressure where it is needed.

I was glad to see that the outgoing director of information technology to say, “Keep the pressure on us.” But how hard do you punch? I mean, do you punch with an answer or do you just punch for the sake of punching because someone has said that we are not where we need to be and the federal statutes call for greater?

So anything that you gentlemen—there is only two of us here—so if there is anything you gentlemen can share with us that, if you were in the position that we are in right now, how could we improve?

That was a question in the last panel, how can we help the department move faster? Congressman Sheila Jackson-Lee asked the question, “Did we do something that we should not have done within the federal act?” And there was legislation filed last session dealing with this subject, and there is legislation, I understand, that will be filed next week dealing with subject, too.

So could you answer along those lines of what you see, as professionals in the area in question?

Mr. ZWILLINGER. Sure. I have two points I think I can try to be helpful with.

The first is that, when we started to try to protect the private-sector information security infrastructure, we started with industry-specific, you know, statutes. We started with Gramm–Leach–Bliley, and we started with HIPAA. And we said financial information is more important. Let us protect that. Health information is more important. Let us protect that.

And then now, and only in 2004, have we had statutes of general applicability trying to get the rest of the country’s information security up to a certain standard.

It seems to me that there is no reason to treat all of the government’s agencies the same. That is, when FISMA was passed, it separately treated national security systems as coming under sort of separate rules.

I do not know—even if you are not a national security system, I still think there is a basis to distinguish between systems that

are so critical to our nation's infrastructure and systems from other agencies that would score lower on the risk scale. And so more time, energy and resources could be devoted to dividing up systems, because it seemed to work in the private sector, to start with financial systems and then move on.

The second point—and I think some of my clients would not like me to sort of admit this honestly, but it is true—is that the public disclosure requirement has really forced companies to spend more money on security than they might have planned, absent that requirement.

That is, they said, “The thing we really do not want to have happen is to have to make a public disclosure of this breach, so then we come vulnerable in the news, our trade value goes down, and the people who might want to sue us get wind of it.” If we could figure out who at DHS, who DHS least wants to disclose security breaches to and force them to do it in the same way the private sector has done it, I would think you would have some of the same incentives of compliance that we see outside.

Mr. MEEK. But know what the unfortunate thing about that? That happens after the fact. I mean, there is some commission, like the 9/11 Commission, that is appointed and then folks start to come forward. “Well, we knew this, but, you know, how do we say it?”

And it is different, I think, for the private sector as it relates to national security. Of course, there is some information of it was stolen that could be very sensitive and could be detrimental to the—you know, could be seen as a security risk for the general public to know. But there has to be some bar.

And I am looking within FISMA to see if such a requirement can, I mean, exist. Because I am pretty sure it is happened, just like it is happened in the private sector. And the more the public knows, the posture that we are in, hopefully, the faster that we can move.

And I do not know if we can legislate that. That is what I am trying to get down to. There has to be a will.

But I do not think folks are sitting around the department saying, “Well, you know, this F means nothing to us, you know? And the public scrutiny within the IT world means nothing to us.”

Because I know professionally in the private sector—Mr. Chairman, if I can—I know that professionally in the private sector that there are associations and groups that work together constantly in concert to make sure that the industry is secured.

I do not know exactly if that is something that formally exists within the public sector. Maybe amongst local governments—I mean, a conference or something. But helping one another to be able to move the ball—because it is an ever-changing issue as it relates to securing information, from what I have read.

Last Congress, I served on the Subcommittee on Cybersecurity, and I started reading some of the publications that were published on it. And it is ever-changing. As you soon as you find the right combination to stop hackers from getting into the system or infiltrating the system, they find a new way to get in.

Mr. MACCARTHY. If I could jump in there for—I think you are right about the notification and other after-the-fact incentives not

being perfect, because they rely on feedback loops. And you know, after the fact, it may be too late.

So I think you need stuff up front. And that is why, when we put in place our program, it was designed to provide good security requirements at the beginning to see if we could make sure that the notification never had to be given because the security was there to begin with.

I have two points. One is, one of the reasons our Visa CISP program is effective is that it is specific. You know, we are not trying to solve all security problems at once. We are focused on one, you know, relatively narrow problem.

It has got a lot of aspects to it, but it is—how do you protect cardholder information? I think to that—if this is a recommendation to the rest of the world, it is find specific security problems and focus on what you think might be important to solve and solve those.

In our experience, you know, two things seem to jump out as being effective. One, we found the role of independent audits to be very, very important. It focuses the attention of people who have to do good security on finding out that there are problems and then enabling them to take remedial steps right away.

The other is, to the extent that we discovered problems with the payment application software where there was security flaws, we worked with outside assessors, discovered those flaws, worked with the vendors. We now have a program of approved, validated payment application software that merchants and other processors can use, which are free of the defects that we found in earlier versions of that kind of software.

So some sort of validation program for software that is used seemed to be a very, very good program, from our point of view. And we think it is the kind of thing that, if you are looking for lessons learned, it is one of the lessons that we learned.

Mr. ROGERS. Thank you, gentlemen, both for your testimony and your answers, and, Mr. Meek, for your questions.

There may be some additional questions that Members have. It is Thursday afternoon, and votes have completed, so they are on airplanes heading home right now. But they may have some additional questions that they will submit to you. I would ask you if you could respond to those in writing, if they do submit them. We are going to leave the record open for 10 days.

For that, I thank you again for your testimony.

And this committee meeting is adjourned.

[Whereupon, at 4:16 p.m., the subcommittee was adjourned.]

