NO COMPUTER SYSTEM LEFT BEHIND: A REVIEW OF THE 2005 FEDERAL COMPUTER SECURITY SCORECARDS

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MARCH 16, 2006

Serial No. 109–139

Printed for the use of the Committee on Government Reform

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

U.S. GOVERNMENT PRINTING OFFICE

27–511 PDF WASHINGTON : 2006

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 GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

CHRISTOPHER SHAYS, Connecticut
DAN BURTON, Indiana
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
GIL GUTKNECHT, Minnesota
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, JR., Tennessee
CANDICE S. MILLER, Michigan
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
JON C. PORTER, Nevada
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. MCHENRY, North Carolina
CHARLES W. DENT, Pennsylvania
VIRGINIA FOXX, North Carolina
JEAN SCHMIDT, Ohio

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. DUTCH RUPPERSBERGER, Maryland
BRIAN HIGGINS, New York
ELEANOR HOLMES NORTON, District of Columbia

BERNARD SANDERS, Vermont (Independent)

DAVID MARIN, *Staff Director*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

CONTENTS

NO COMPUTER SYSTEM LEFT BEHIND: A REVIEW OF THE 2005 FEDERAL COMPUTER SECURITY SCORECARDS

THURSDAY, MARCH 16, 2006

HOUSE OF REPRESENTATIVES,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The committee met, pursuant to notice, at 12:16 p.m., in room 2154, Rayburn House Office Building, Hon. Tom Davis (chairman of the committee) presiding.

Present: Representatives Tom Davis, Platts, Cummings, Clay, and Watson.

Staff present: David Marin, staff director; Keith Ausbrook, chief counsel; Chas Phillips, policy counsel; Rob White, press secretary; Drew Crockett, deputy director of communication; Victoria Proctor, senior professional staff member; Teresa Austin, chief clerk; Sarah D'Orsie, deputy clerk; Leneal Scott, computer systems manager; Michael McCarthy, minority counsel; Earley Green, minority chief clerk; and Jean Gosa, minority assistant clerk.

Chairman TOM DAVIS. Good afternoon and welcome. The committee will come to order.

Today, the committee is releasing its Federal computer security scorecards and will examine the status of agency compliance with the Federal Information Security Management Act [FISMA].

Information technology and the Internet drive our economy and help the Federal Government to operate with greater efficiency and cost savings. E-commerce, information sharing, and Internet transactions, such as online tax filings, are so common that we take them for granted. Not until an incident such as the potential BlackBerry shutdown—which was recently settled—are we reminded of our dependence on IT and how difficult it is for us to function without it.

In the past year or so, we have heard stories about identity theft, security breaches in large commercial data bases, and phishing scams such as those identified by the Internal Revenue Service this tax season. We have also seen an increase in education and awareness campaigns for online safety spearheaded by the private and public sectors. But in my experience, when it comes to Federal IT policy and information security, it is still difficult to get people—even Members of Congress—engaged. For most people this is an abstract, inside-the-Beltway issue. And FISMA is still viewed by some Federal agencies as a paperwork exercise. But these are short-sighted observations. As a result of the Government's aggres-

sive push to advance e-government, many Government information systems hold personal information about citizens and employees, in addition to other types of data. Maintaining the integrity, privacy, and availability of all information in these systems is vital to our national security, continuity of operations, and economy.

Furthermore, in order to successfully fight the war on terror, we must be able to move information to the right people at the right place at the right time. Information needs to move seamlessly, securely, and efficiently within agencies, across departments, and across jurisdictions of Government as well.

Due to the nature of our cyber infrastructure, an attack could originate anywhere at any time. We know that Government systems are prime targets for hackers, terrorists, hostile foreign governments, and identity thieves. Malicious or unintended security threats come in varied forms: denial of service attacks, malware, worms and viruses, phishing scams, and software weaknesses, to just name a few. Any of these threats can compromise our information systems. The results can be costly, disruptive, and erode public trust in Government.

One of the best ways to defend against attacks is to have a strong, yet flexible, protection policy in place. We want agencies to actively protect their systems instead of just reacting to the latest threat with patches and other responses. FISMA accomplishes this goal by requiring each agency to create a comprehensive risk-based approach to agency-wide information security management. FISMA strengthens Federal cyber preparedness, evaluation, and reporting requirements. It is intended to make security management an integral part of an agency's operations and to ensure that we are actively using best practices to secure our systems and prevent devastating damage.

The committee, with technical assistance from GAO, releases annual scorecards based on the FISMA reports submitted to us by agency Chief Information Officers and Inspectors General. This year, the Federal Government as a whole hardly improved, receiving a D+ yet again. Our analysis reveals that the scores for the Departments of Defense, Homeland Security, Justice, State—the agencies on the front lines in the war on terror—remained unacceptably low or in some cases dropped precipitously. Meanwhile, several agencies improved their information security or maintained a consistently high level of security from previous years.

The 2005 FISMA grades indicate that agencies have made improvements in developing configuration management plans, employee security training, developing and maintaining an inventory, certifying and accrediting systems, and annual testing. Despite these advances, there are still some areas of concern to the committee, including implementation of configuration management policies, specialized security training for employees with significant security responsibilities, inconsistent incident reporting, inconsistencies in contingency plan testing, annual testing of security controls, and agency responsibility for contractor systems.

At today's hearing, we will evaluate the results of the agencies' 2005 FISMA reports, identify strengths and weaknesses in Government information security, and learn whether FISMA provisions and the OMB guidance are sufficient to help secure Government

information systems. Witnesses from GAO and OMB will help us understand what obstacles impede the Government's ability to comply with FISMA. DOD and DHS witnesses will discuss the challenges they face in their departments and their plans to improve FISMA compliance. We will also hear about best practices and lessons learned from the Social Security Administration and Department of Labor, two agencies that have demonstrated consistent improvements in their information security since the scorecard process was initiated in 2001.

If FISMA was the No Child Left Behind Act, a lot of critical agencies would be part of the list of low performers. None of us would accept D+ grades on our children's report cards. We can't accept these either.

[The prepared statement of Chairman Tom Davis follows:]

Oversight Hearing

"No Computer System Left Behind: A Review of the 2005 Federal Computer Security Scorecards"

Thursday, March 16, 2006
10:00 a.m.
Room 2154 Rayburn House Office Building

Opening Statement

Good morning and welcome. A quorum being present, the Committee on Government Reform will come to order. Today, the Committee is releasing its federal computer security scorecards and will examine the status of agency compliance with the Federal Information Security Management Act (FISMA).

Information technology and the Internet drive our economy and help the federal government operate with greater efficiency and cost savings. E-commerce, information sharing, and Internet transactions, such as online tax filing, are so commonplace that we take them for granted. Not until an incident such as the potential Blackberry shutdown – which was recently settled – are we reminded of our dependence on IT and how difficult it is for us to function without it.

In the past year or so, we have heard stories about identity theft, security breaches in large commercial databases, and phishing scams such as those identified by the Internal Revenue Service this tax season. We have also seen an increase in education and awareness campaigns for online safety spearheaded by the private and public sectors. But in my experience, when it comes to *federal* IT policy and information security, it is still difficult to get people – even members of Congress – engaged. For most people this is an abstract, inside-the-Beltway issue. And FISMA is still viewed by some federal agencies as a paperwork exercise. But these are short-sighted observations. As a result of the government's aggressive push to advance e-government, many government information systems hold personal information about citizens and employees, in addition to other types of data. Maintaining the integrity, privacy, and availability of all information in these systems is vital to our national security, continuity of operations, and economy.

Furthermore, in order to successfully fight the war on terror, we must be able to move information to the right people at the right place and time. Information needs to move seamlessly, securely, and efficiently within agencies, across departments, and across jurisdictions of government as well.

Due to the nature of our cyber infrastructure, an attack could originate anywhere at any time. We know that government systems are prime targets for hackers, terrorists, hostile foreign governments, and identity thieves. Malicious or unintended security threats come in varied forms: denial of service attacks, malware, worms and viruses, phishing scams,

and software weaknesses, to name a few. Any of these threats can compromise our information systems. The results would be costly, disruptive, and erode public trust in government.

One of the best ways to defend against attacks is to have a strong, yet flexible, protection policy in place. We want agencies to actively protect their systems instead of just reacting to the latest threat with patches and other responses. FISMA accomplishes this goal by requiring each agency to create a comprehensive risk-based approach to agency-wide information security management. FISMA strengthens Federal cyber preparedness, evaluation, and reporting requirements. It's intended to make security management an integral part of an agency's operations, and to ensure that we are actively using best practices to secure our systems and prevent devastating damage.

The Committee, with technical assistance from GAO, releases annual scorecards based on the FISMA reports submitted to us by agency Chief Information Officers and Inspectors General. This year, the federal government as a whole hardly improved, receiving a D+ yet again. Our analysis reveals that the scores for the Departments of Defense, Homeland Security, Justice, State – the agencies on the front line in the war on terror - remained unacceptably low or dropped precipitously. Meanwhile, several agencies improved their information security or maintained a consistently high level of security from previous years.

The 2005 FISMA grades indicate that agencies have made improvements in developing configuration management plans, employee security training, developing and maintaining an inventory, certifying and accrediting systems, and annual testing. Despite these advances, there are still some areas of concern to the Committee, including implementation of configuration management policies, specialized security training for employees with significant security responsibilities, inconsistent incident reporting, inconsistencies in contingency plan testing, annual testing of security controls, and agency responsibility for contractor systems.

At today's hearing, we will evaluate the results of the agencies' 2005 FISMA reports, identify strengths and weaknesses in government information security, and learn whether FISMA provisions and the OMB guidance are sufficient to help secure government information systems. Witnesses from GAO and OMB will help us understand what obstacles impede the government's ability to comply with FISMA. DOD and DHS witnesses will discuss the challenges they face in their departments and their plans to improve FISMA compliance. We will also hear about best practices and lessons learned from the Social Security Administration and Department of Labor, two agencies that have demonstrated consistent improvements in their information security since the scorecard process was initiated in 2001.

If FISMA was the No Child Left Behind Act, a lot of critical agencies would be on the list of "low performers." None of us would accept D+ grades on our children's report cards. We can't accept these either.

Chairman TOM DAVIS. Are there any other Members who wish to make opening statements? If not, I am going to note that Members will have 7 days to submit opening statements for the record.

We are going to recognize our first panel of distinguished witnesses. We have Mr. Gregory Wilshusen, the Director of Information Security Issues for the U.S. Government Accountability Office, and the Honorable Karen Evans, the Administrator of the Office of E-Government and Information Technology at the Office of Management and Budget. You know it is our policy we swear you in before your testimony, so if you would just rise and raise your right hands.

[Witnesses sworn.]

Chairman TOM DAVIS. Thank you. Let me thank you for your perseverance on this.

Mr. Wilshusen, thank you for being with us.

STATEMENTS OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; AND KAREN S. EVANS, ADMINISTRATOR, OFFICE OF ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET

STATEMENT OF GREGORY WILSHUSEN

Mr. WILSHUSEN. Thank you, Mr. Chairman.

I am pleased to be here once again to discuss the efforts by Federal agencies to implement the requirements of FISMA. For many years, we have reported that inadequate information security is a widespread problem that could have devastating consequences. Since 1997, we have identified information security as a government-wide high-risk issue.

Today, the Federal Government is facing increasingly sophisticated and complex threats to its sensitive information systems and information. The need for agencies to implement the strong information security controls required by FISMA has never been greater.

My testimony is based, in part, on our analysis of the fiscal year 2005 FISMA reports by OMB and 24 major Federal agencies and their Inspectors General.

Mr. Chairman, my bottom-line message is that progress made by the agencies in implementing FISMA is mixed, at best. Agencies have made progress in several areas but have slipped in others.

Today, I will note areas where agencies have made progress and those areas where weaknesses remain. In addition, I will discuss actions that agencies can take to improve their information security controls.

Before I do, I would like to recognize OMB for taking steps to improve the quality of the FISMA reports. For example, OMB required agencies to report, for the first time, certain performance measures by system risk level. This provides better information about whether agencies are prioritizing their information security efforts according to system risk.

Mr. Chairman, agency FISMA reports present a mixed picture of FISMA implementation. The agencies generally reported an increasing number of systems meeting key security performance

measures, such as the percentage of systems certified and accredited, and the percentage of contingency plans tested.

Nevertheless, progress was uneven. For example, the percentage of agency systems reviewed declined from 96 percent in 2004 to 84 percent in 2005, and the percentage of employees and contractors receiving security awareness training also declined.

The reports indicated other challenges as well. Only 13 IGs reported that their agencies' inventories of major systems were substantially complete. A complete inventory is a key element of managing the agency's IT resources, including the security of those resources. Without complete inventories, the agencies, the administration, and the Congress cannot be fully assured of the agencies' progress in implementing FISMA.

Eight IGs also assessed the quality of their agency's certification and accreditation processes as "poor." As a result, agency-reported performance data may not accurately reflect the status of the agency's efforts to implement this requirement.

And 39 percent of Federal systems did not have a tested contingency plan. Without a tested plan, increased risk exists that agencies will not be able to recover mission-critical systems in a timely manner if an interruption occurs.

Beyond assessing FISMA requirements, our audits of information security at Federal agencies have found significant weaknesses related to access controls and other information security controls that place a broad array of Federal operations and assets at risk of misuse and disruption.

However, agencies can take several actions to fully implement their FISMA-mandated programs and improve security controls. Such actions include completing and maintaining accurate inventories of major systems, prioritizing information security efforts based on system risk levels, and strengthening controls that are to prevent, limit, and detect access to its information and information systems.

Mr. Chairman, this concludes my statement. I will be happy to answer your questions.

[The prepared statement of Mr. Wilshusen follows:]

United States Government Accountability Office

GAO

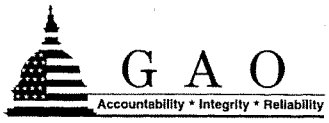
Testimony
Before the House Committee on Government Reform

For Release on Delivery
Expected at 10:00 a.m. EST
Thursday, March 16, 2006

INFORMATION SECURITY

Federal Agencies Show Mixed Progress in Implementing Statutory Requirements

Statement of Gregory C. Wilshusen
Director, Information Security Issues



GAO-06-527T

March 16, 2006

GAO
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-06-527T, a testimony to the House Committee on Government Reform

INFORMATION SECURITY

Federal Agencies Show Mixed Progress in Implementing Statutory Requirements

Why GAO Did This Study

For many years, GAO has reported that ineffective information security is a widespread problem that has potentially devastating consequences. In its reports to Congress since 1997, GAO has identified information security as a governmentwide high-risk issue—most recently in January 2005.

Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, Congress passed the Federal Information Security Management Act of 2002 (FISMA), which permanently authorized and strengthened the federal information security program, evaluation, and reporting requirements established for federal agencies.

This testimony discusses:

- The federal government's progress and challenges in implementing FISMA, as reported by the Office of Management and Budget (OMB), the agencies, and the Inspectors General (IGs).
- Actions needed to improve FISMA reporting and address underlying information security weaknesses.

www.gao.gov/cgi-bin/getrpt?GAO-06-527T.

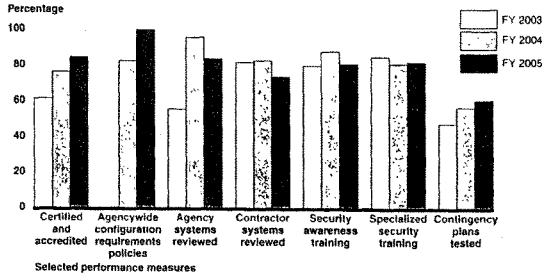
To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

In its fiscal year 2005 report to Congress, OMB discusses progress in implementing key information security requirements, but at the same time cites challenging weaknesses that remain. The report notes several governmentwide findings, such as the varying effectiveness of agencies' security remediation processes and the inconsistent quality of agencies' certification and accreditation (the process of authorizing operation of a system, including the development and implementation of risk assessments and security controls). Nevertheless, fiscal year 2005 data reported by 24 major agencies, compared with data reported for the previous 2 fiscal years (see fig.), show that these agencies have made steady progress in certifying and accrediting systems, although they reported mixed progress in meeting other key statutory information security requirements. For example, agencies reported that only 61 percent of their systems had tested contingency plans, thereby reducing assurance that agencies will be able to recover from the disruption of those systems with untested plans.

Federal entities can act to improve the usefulness of the annual FISMA reporting process and to mitigate underlying information security weaknesses. OMB has taken several actions to improve FISMA reporting—such as requiring agencies to provide performance information based on the relative importance or risk of the systems—and can further enhance the reliability and quality of reported information. Agencies also can take actions to fully implement their FISMA-mandated programs and address the weaknesses in their information security controls. Such actions include completing and maintaining accurate inventories of major systems, prioritizing information security efforts based on system risk levels, and strengthening controls that are to prevent, limit, and detect access to the agencies' information and information systems.

Reported Data for Selected Performance Measures for 24 Major Agencies



Source: GAO analysis of agencies' FY2003-2005 FISMA reports.

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss the state of federal information security and the efforts by federal agencies 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] Since 1997, we have identified information security as a governmentwide high-risk issue in reports to the Congress.[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.

In my testimony today, I will summarize our analysis of the reported status of the federal government's implementation of FISMA. I will note areas where the agencies have made progress in implementing the requirements of the Act and those areas where weaknesses remain. I will also touch on additional actions that federal entities can take to help fully implement the mandated information security programs and to improve the effectiveness of information security controls.

In conducting this work, we reviewed and summarized OMB's fiscal year 2005 report to Congress on FISMA implementation, dated March 1, 2006. We also analyzed and summarized the fiscal year

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

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

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

2005 FISMA reports from 24 major federal agencies[4] and their inspectors general (IGs). In addition, we reviewed standards and guidance issued by OMB and the National Institute of Standards and Technology (NIST) pursuant to their responsibilities under the Act. We did not validate the accuracy of the data reported by the agencies or OMB, but we did analyze the IGs' fiscal year 2005 FISMA reports to identify any issues related to the accuracy of agency-reported information. Finally, we examined and summarized key findings of related GAO products. We performed our work from October 2005 to March 2006 in accordance with generally accepted government auditing standards.

Results in Brief

In its fiscal year 2005 report to the Congress, OMB noted that the federal government has made progress in meeting key performance measures for information security; however, uneven implementation of security efforts has left weaknesses in several areas. OMB identified weaknesses with the extent of agencies' oversight of contractor systems, testing of security controls, and reporting of security incidents, as well as the quality of agencies' plans of action and milestones and certification and accreditation processes. The report presented a plan of action that OMB is pursuing with federal agencies to improve their management of information security.

The fiscal year 2005 reports submitted by the agencies present a mixed picture of FISMA implementation in the federal government. In their fiscal year 2005 reports, 24 major federal agencies generally reported an increasing number of systems meeting key information security performance measures, such as percentage of systems certified and accredited and percentage of contingency plans tested.

[4] These 24 departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, and, Veterans Affairs, the Environmental Protection Agency, General Services Administration, Office of Personnel Management, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

Nevertheless, progress was uneven. For example, the percentage of agency systems reviewed declined from 96 percent in 2004 to 84 percent in 2005, and the percentage of employees and contractors receiving security awareness training also declined, from 88 percent in 2004 to 81 percent in 2005.

Federal entities can act to improve the usefulness of the annual FISMA reporting process and to mitigate underlying information security weaknesses. OMB has taken several actions to improve FISMA reporting — such as requiring agencies to indicate the relative importance or risk level of their systems — and can further enhance the reliability and quality of reported information. Agencies can also take actions to fully implement their FISMA-mandated programs and address the weaknesses in their information security controls. Such actions include completing and maintaining accurate inventories of major systems, prioritizing information security efforts based on system risk levels, and strengthening controls that are designed to prevent, limit, and detect access to the agencies' information and information systems.

Background

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 this interconnectivity offers us huge benefits, without proper safeguards it also poses significant risks to the government's computer systems and, more importantly, to the critical operations and infrastructures they support. We reported in 2005 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.[5]

The significance of these weaknesses led us to conclude in the audit of the federal government's fiscal year 2005 financial statements[6] that information security was a material weakness.[7] Our audits also identified instances of similar types of weaknesses in non-financial systems.

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 we 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 other computer systems.
- 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.

[5]GAO, *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, GAO-05-552 (Washington, D.C.: July 15, 2005).

[6]GAO, *Fiscal Year 2005 U.S. Government Financial Statements: Sustained Improvement and Financial Management is Crucial to Addressing our Nation's Financial Conditions and Long-term Fiscal Imbalance*, GAO-06-406T (Washington, D.C.: March 1, 2006).

[7]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.

- Data could be modified or destroyed for purposes of fraud, identity theft, or disruption.
- Agency missions could be undermined by embarrassing incidents that result in diminished confidence in federal organizations' abilities to conduct operations and fulfill their fiduciary responsibilities.

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. The Act 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 (including agencies with national security systems) to develop, document, and implement an agencywide information security program. This program should provide 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, including minimally acceptable system configuration requirements;

- 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 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 (including major national security systems) that are operated by the agency or 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 must submit a report to the Congress no later than March 1 of each year on agency compliance, including a summary of the findings of agencies' independent evaluations.

Other major provisions direct that the National Institute of Standards and Technology (NIST) 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 of and guidelines concerning detection and handling of information security incidents and guidelines.

OMB Reporting Instructions and Guidance Emphasize Performance Measures

OMB provides instructions to the agencies and their IGs on the annual FISMA reporting requirements. OMB's fiscal year 2005 reporting instructions, similar to the 2004 instructions, have a strong focus on performance measures. OMB has developed performance measures in the following areas:

- certification and accreditation,[8]
- testing of security controls,
- agency systems and contractor systems reviewed annually,
- testing of contingency plans,
- incident reporting,

[8]Agency management officials are required to 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.

- annual security awareness training for employees and contractors,
- annual specialized training for employees with significant security responsibilities, and
- minimally acceptable configuration requirements.

Further, OMB has 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 to OMB. In addition, agencies are to submit quarterly updates that indicate the number of weaknesses for which corrective action has been completed as originally scheduled, or has been delayed, as well as the number of new weaknesses discovered since the last update.

The annual IGs' reports requested by OMB are to be based on the results of their independent evaluations, including work performed throughout the reporting period (such as work performed as part of the annual financial audits of the agencies). While OMB asked the IGs to respond to some of 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 quality of the certification and accreditation process at their agencies, as well as the status of their agency's inventory of major information systems. 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.

OMB's Report to the Congress Noted Improvements and Weaknesses

In its March 2006 report to the Congress on fiscal year 2005 FISMA implementation,[9] OMB emphasized that the federal government has made progress in meeting key performance measures for IT security; however, uneven implementation of security efforts leaves weaknesses in several areas. OMB determined through its assessment of FISMA reports that advances have occurred at a governmentwide level in the following areas of IT security:

- *Systems certification and accreditation.* Agencies recorded a 19 percent increase in the total number of IT systems and reported that the percentage of certified and accredited systems rose from 77 percent in fiscal year 2004 to 85 percent in 2005. Moreover, OMB noted that 88 percent of systems assessed as high-risk have been certified and accredited.
- *Assessed quality of the certification and accreditation process.* OMB's analysis of reports from the IGs revealed an increase in agencies with a certification process rated as "satisfactory" or higher, from 15 in 2004 to 17 in 2005.
- *Plans of action and milestone process.* OMB noted that out of 25 agencies that it reviewed in detail,[10] 19 IGs report that their agencies have effective remediation processes, compared to 18 in 2004.

In addition to these areas of improvement, OMB detected areas with continuing weaknesses:

- *Contractor systems oversight.* IGs for 6 of 24 agencies (one agency IG did not respond) rated agency oversight of contractor systems in the "rarely" range, while 3 others rated this oversight in the next lowest range, "sometimes."

[9]Office of Management and Budget, *FY2005 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002* (Washington, D.C.: March, 2006).

[10]OMB includes the Smithsonian Institution in its list of major agencies. Our analysis in this testimony does not include the Smithsonian Institution.

- *Security controls testing.* Agencies tested the security controls on a lower percentage of systems, dropping from 76 percent in fiscal year 2004 to 72 percent in 2005. OMB noted a better rate of testing for high-risk systems, with a governmentwide total of 83 percent.
- *Incident reporting.* OMB stated that some agencies continue to report security incidents to the Department of Homeland Security only sporadically and that others report notably low levels of incidents.
- *Agencywide plans of action and milestones.* While IGs for 19 agencies reported effective POA&M processes, 6 others reported ineffective processes.
- *Certification and accreditation process.* OMB commented that while no IG rated the certification and accreditation process for its agency as failing, eight rated the process as "poor."

The OMB report also discusses a plan of action to improve performance, assist agencies in their information security activities, and promote compliance with statutory and policy requirements. OMB has set a goal for agencies to have 90 percent of their systems certified and accredited and their certification and accreditation process rated as "satisfactory" or better by their IGs.

Agency 2005 FISMA Reports Show Mixed Results

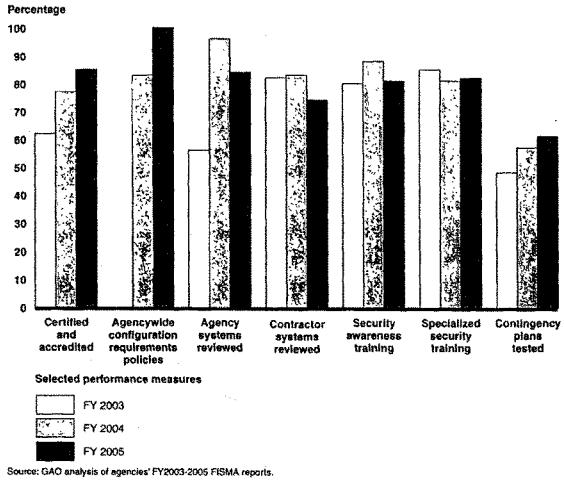
In their FISMA-mandated reports for fiscal year 2005, the 24 major agencies reported both improvements and weaknesses in major performance indicators. The following key measures showed increased performance and/or continuing challenges:

- percentage of systems certified and accredited;
- percentage of agencies with an agencywide minimally acceptable configuration requirements policy;
- percentage of agency systems reviewed annually;
- percentage of contractor systems 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 contingency plans tested.

Figure 1 illustrates that the major agencies have made steady progress in fiscal year 2005 certifying and accrediting their systems, although they have made mixed progress in meeting other key performance measures compared with the previous two fiscal years. Summaries of the results for specific measures follow.

Figure 1: Reported Data for Selected Performance Measures for 24 Major Agencies



Source: GAO analysis of agencies' FY2003-2005 FISMA reports.

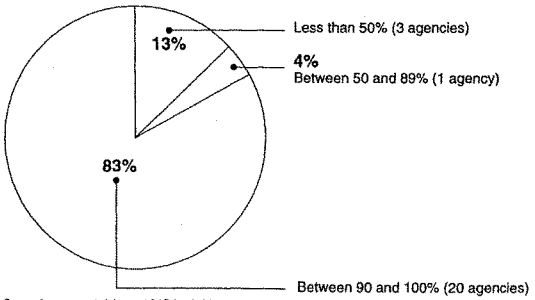
Certification and Accreditation

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. For FISMA reporting, OMB requires agencies to report the number of systems authorized for processing after completing certification and accreditation.

Data reported for this measure showed continued overall increases for most agencies over the last three years. For example, 15 agencies reported an increase in the percentage of their systems that had completed certification and accreditation. Overall, 85 percent of agencies' systems governmentwide were reported as certified and accredited in 2005, compared to 77 percent in 2004 and 62 percent in 2003. In addition, 20 agencies reported that 90 percent or more of their systems had successfully completed the process, as illustrated in figure 2.

Figure 2: Percentage of Agencies Reporting the Percentage of Their Systems that are Certified and Accredited for Processing in Fiscal Year 2005



Source: Agency-reported data and GAO (analysis).

Agencies appeared to appropriately focus their certification and accreditation efforts on high-risk systems. Agencies certified and

accredited a higher percentage of their high-risk systems (88 percent) than their moderate-risk systems.

Configuration Management

FISMA requires each agency to have policies and procedures that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. In fiscal year 2004, for the first time, agencies reported on the degree to which they had security configurations for specific operating systems and software applications. Our analysis of the 2005 agency FISMA reports found that all 24 major agencies reported that they had agencywide policies containing system configurations, an increase from the 20 agencies who reported having them in 2004. However, implementation of these requirements at the system level continues to be uneven. Specifically, 14 agencies reported having system configuration policies, but they did not always implement them on their systems.

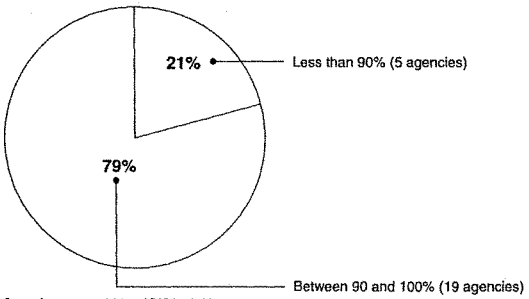
Annual Review of Agency Systems

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 effort is to include testing of management, operational, and technical controls of 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. In order to measure the performance of security programs, OMB requires that agencies report the number and percentage of systems that they have reviewed during the year.

Agencies reported a decrease in the percentage of their systems that underwent an annual review in 2005, after reporting major gains in this performance measure in 2004. In the 2005 reports, agencies stated that 84 percent of their systems had been reviewed in the last

year, as compared to 96 percent in 2004. While 23 agencies reported that they had reviewed 90 percent or more of their systems in 2004, 19 agencies reported this achievement in 2005, as shown in figure 3.

Figure 3: Percentage of Agencies Reporting the Percentage of Their Systems that have been Reviewed in Fiscal Year 2005



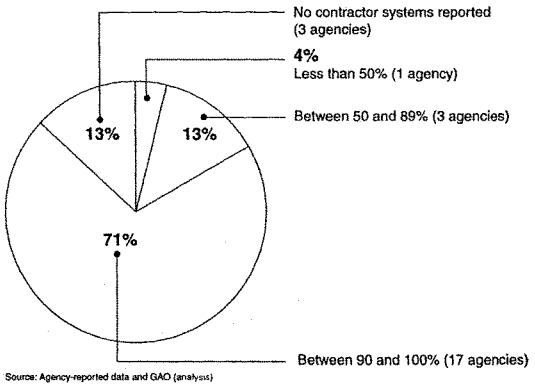
Source: Agency-reported data and GAO (analysis).

Annual Review of Contractor Systems

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. As OMB emphasized in its fiscal year 2005 FISMA reporting guidance, agency IT 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. Such other organizations may include contractors, grantees, state and local governments, and industry partners. According to 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.

The key performance measure of annual review of contractor systems by agencies decreased from 83 percent in 2004 to 74 percent in 2005, reducing the rate of reviews performed to below 2003 levels. However, the number of agencies that reported reviewing over 90 percent of their contractor systems has increased from 10 in 2004 to 17 in 2005. A breakdown of the percentages for fiscal year 2005 is provided in figure 4.

Figure 4: Percentage of Agencies Reporting the Percentage of Their Contractor Systems that have been Reviewed in Fiscal Year 2005



Source: Agency-reported data and GAO (analysis)

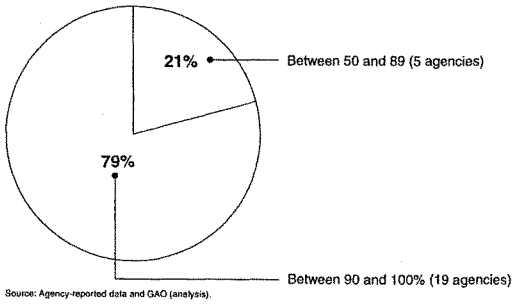
Although agencies reported that 74 percent of their contractor systems were reviewed in 2005, they only reviewed 51 percent of the contractor systems assessed as high-risk, as opposed to 89 percent of moderate-risk systems and 84 percent of low-risk systems. Without adequate contractor review, agencies cannot be assured that federal information held and processed by contractors is secure.

Security Awareness Training

FISMA requires agencies to provide security awareness training. This training should inform personnel, including contractors and other users of information systems supporting the operations and assets of an agency, of information security risks associated with their activities and of the agency's responsibilities in complying with policies and procedures designed to reduce these risks. Our studies of best practices at leading organizations[11] have shown that such organizations took steps to ensure that personnel involved in various aspects of information security programs had the skills and knowledge they needed.

In their FISMA submissions for fiscal year 2005, agencies reported that they provided security awareness training to the majority of their employees and contractors. However, while 19 agencies reported that they had trained more than 90 percent of their employees and contractors in basic security awareness (see fig. 5), the overall percentage of employees trained among the 24 major federal agencies reviewed dropped from 88 percent in 2004 to 81 percent in 2005, a level almost equal to that reported in 2003.

Figure 5: Percentage of Agencies Reporting the Level of Their Employees and Contractors that have Received IT Security Awareness Training in Fiscal Year 2005



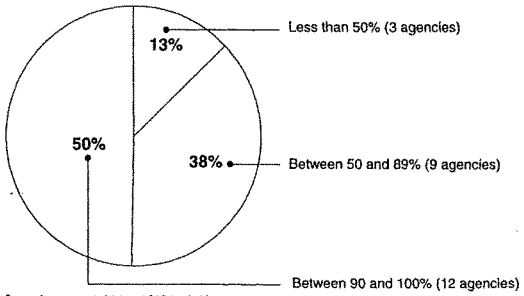
Source: Agency-reported data and GAO (analysis).

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 current on changes in threats, vulnerabilities, software, technologies, security techniques, and security monitoring tools. OMB directs agencies to report on the percentage of their employees with significant security responsibilities who have received specialized training.

Agencies reported varying levels of compliance in providing specialized training to employees with significant security responsibilities. Of the 24 agencies that we reviewed, 12 reported that they had provided specialized security training for 90 percent or more of these employees. (see fig. 6).

Figure 6: Percentage of Agencies Reporting the Level of Their Employees with Significant Security Responsibilities that have Received Specialized Security Training in Fiscal Year 2005



Source: Agency-reported data and GAO (analysis).

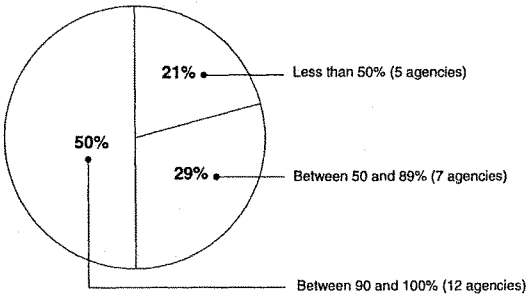
Although there was a gain of one point in the percentage of employees who received specialized security training for fiscal year 2005 (82 percent) over 2004 (81 percent), both of these years show a decrease from the level reported in 2003 (85 percent). Given the rapidly changing threats in information 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 a temporary power failure, the 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 the plans will function as intended in an emergency, and the frequency of plan testing will vary depending on the criticality of the entity's operations. The most useful tests involve simulating a disaster to test overall service continuity. Such a test includes testing whether the alternative data processing site will function as intended and whether critical computer data and programs to be recovered from off-site storage will be accessible and current. In executing the plan, managers are able to identify weaknesses and make changes accordingly. Moreover, such tests assess how well employees have been trained to carry out their roles and responsibilities during a disaster. To show the status of implementing this requirement, OMB specifies that agencies report the number of systems with tested contingency plans.

Overall, agencies continued to report that they have not tested a significant number of their contingency plans with only 61 percent of systems with tested plans. Although this number continues to show small increases each year since 2003, figure 7 illustrates that 5 agencies reported less than 50 percent of their systems had tested contingency plans.

Figure 7: Percentage of Agencies Reporting the Level of Their Systems that have Tested Contingency Plans in Fiscal Year 2005



Source: Agency-reported data and GAO (analysis).

In addition, agencies do not appear to be appropriately prioritizing testing of contingency plans by system risk level, with high-risk systems having the lowest rate of systems with tested plans of the three risk levels. 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.

Inventory of Major Systems

FISMA requires that agencies develop, maintain, and annually update an inventory of major information systems operated by the agency, or under its control. 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. For the 2005 reports, OMB required agencies to report the number of major systems and asked the IGs about the status and accuracy of their agencies' inventories.

In 2005, agencies reported 10,261 systems, composed of 9,175 agency systems and 1,094 contractor systems. However, only 13 IGs reported that their agencies' inventories were substantially complete. A complete inventory of major information systems is a key element of managing the agency's IT resources, including the security of those resources. Without reliable information on agencies' inventories, the agencies, the administration, and Congress cannot be fully assured of agencies' progress in implementing FISMA.

Risk Assessments

FISMA mandates that agencies assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure disruption, modification, or destruction of their information and information systems. The Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, and related NIST guidance provide a common framework for categorizing systems according to risk. The framework establishes three levels of potential impact on organizational operation, assets, or individuals should a breach of security occur—high (severe or catastrophic), moderate (serious), and low (limited)—and is used to determine the impact for each of the FISMA-specified security objectives of confidentiality, integrity, and availability. Once determined, security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. OMB's fiscal year 2005 reporting instructions included the new requirement that agencies report their systems and certain performance measures using FIPS 199 risk levels. If agencies did not categorize systems, or used a method other than FIPS 199 to determine risk level, they were required to explain why in their FISMA reports.

For the first time, in the 2005 reporting, agencies reported the risk levels for their agency and contractor systems, as illustrated in table 1.

Table 1: Systems Reported by Risk Level in Fiscal year 2005

Risk Level	Agency Systems	Percentage	Contractor Systems	Percentage	Overall Percentage
High-risk	1,646	18	293	27	19
Moderate-risk	2,493	27	249	23	27
Low-risk	4,446	49	164	15	45
Not categorized	580	6	390	35	9
Totals	9,165	100	1,096	100	100

Source: GAO analysis.

Agencies reported that 9 percent of their systems were not categorized by risk level. The majority of systems without risk levels assigned were found at 4 agencies. One agency did not categorize 77 percent of its systems. Without assigned risk levels, agencies cannot make risk-based decisions on the security needs of their information and information systems.

Actions are Needed to Improve FISMA Reporting and Underlying Information Security Weaknesses

There are actions that OMB and the agencies can take to improve FISMA reporting and compliance and to address underlying weaknesses in information security controls. In our July 2005 report,[12] we evaluated the adequacy and effectiveness of agencies' information security policies and practices and the federal government's implementation of FISMA requirements. We recommended that the Director of OMB take actions in revising future FISMA reporting instructions to increase the usefulness of the agencies' annual reports to oversight bodies by:

- requiring agencies to report FISMA data by risk category;
- reviewing guidance to ensure the clarity of instructions;
- requesting the IGs report on the quality of additional agency processes, such as the annual system reviews.

[12]GAO-05-552

These recommendations were designed to strengthen reporting under FISMA by encouraging more complete information on the implementation of agencies' information security programs.

Consistent with our recommendation, OMB required agencies to report certain performance measures by system risk level for the first time in fiscal year 2005. As a result, we were able to identify potential areas of concern in the agencies' implementation of FISMA. For example, agencies do not appear to be prioritizing certain information security control activities, such as annual review of contractor systems or testing of contingency plans, based on system risk levels. For both of these activities, federal implementation of the control is lower for high-risk systems than it is for moderate or low-risk systems.

OMB has also taken steps to increase the clarity of instructions in their annual guidance. It has removed several questions from prior years that could have been subject to differing interpretations by the IGs and the agencies. Those questions related to agency inventories and to plans of actions and milestones. In addition, OMB clarified reporting instructions for minimally acceptable configuration requirements. The resulting reports are more consistent and, therefore, easier to analyze and compare.

However, opportunities still exist to enhance reporting on the quality of the agencies' information security-related processes. The qualitative assessments of the certification and accreditation process and the plans of actions and milestones have greatly enhanced Congress', OMB's, and our understanding of the implementation of these requirements at the agencies. Additional information on the quality of agencies' processes for annually reviewing or testing systems, for example, could improve understanding of these processes by examining whether federal guidance is applied correctly, or whether weaknesses discovered during the review or test are tracked for remediation. Extending qualitative assessments to additional agency processes could improve the information available on agency implementation of information security requirements.

Federal Agencies Need to Take Actions to Increase FISMA Compliance and Address Already Identified Information Security Weaknesses

Agencies need to take action to implement the information security management program mandated by FISMA and use that program to address their outstanding information security weaknesses. An agencywide security program provides a framework and continuing cycle of activities for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, or improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

As we have previously reported,[13] none of the 24 major agencies has fully implemented agencywide information security programs as required by FISMA. Agencies often did not adequately assess risks, develop sufficient risk-based policies or procedures for information security, ensure that existing policies and procedures were implemented effectively, or monitor operations to ensure compliance and determine the effectiveness of existing controls. Moreover, as demonstrated by the 2005 FISMA reports, many agencies still do not have complete and accurate inventories of their major systems. Until agencies effectively and fully implement agencywide information security programs, federal data and systems will not be adequately safeguarded against unauthorized use, disclosure, and modification.

Agencies need to take action to implement and strengthen their information security management programs. Such actions should include completing and maintaining an accurate, complete inventory of major systems, and prioritizing information security efforts based on system risk levels. Strong incident procedures are necessary to detect, report, and respond to security incidents effectively.

[13]GAO-05-552

Agencies also should implement strong remediation processes that include processes for planning, implementing, evaluating, and documenting remedial actions to address any identified information security weaknesses. Finally, agencies need to implement risk-based policies and procedures that efficiently and effectively reduce information security risks to an acceptable level.

Even as federal agencies are working to implement information security management programs, they continue to have significant control weaknesses in their computer systems that threaten the integrity, reliability, and availability of federal information and systems. In addition, these weaknesses place financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

The weaknesses appear in both access controls and other information security controls defined in our audit methodology for performing information security evaluations and audits.[14] These areas are (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) software change controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations, and (5) an agencywide security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.

In the 24 major agencies' fiscal year 2005 reporting regarding their financial systems, 6 reported information security as a material

[14]GAO, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (Washington, D.C.: January 1999). This methodology is used for our information security controls evaluations and audits, as well as by the IGs for the information security control work done as part of financial audits at the agencies.

weakness and 14 reported it as a reportable condition.[15] Our audits also identified similar weaknesses in nonfinancial systems. In our prior reports, we have made specific recommendations to the agencies to mitigate identified information security weaknesses. The IGs have also made specific recommendations as part of their information security review work.

Agencies Should Address Weaknesses in Access Controls

Agencies would benefit from addressing common weaknesses in access controls. As we have previously reported, the majority of the 24 major agencies had access control weaknesses.[16] A basic management control objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modification, disclosure, or deletion of the data. Based on our previous work performing information security audits, agencies can take steps to enhance the four basic areas of access controls:

- *User identification and authentication.* To enable a computer system to identify and differentiate users so that activities on the system can be linked to specific individuals, agencies assign unique user accounts to specific users, a process called identification. Authentication is the method or methods by which a system establishes the validity of a user's claimed identity. Agencies need to implement strong user identification and authentication controls.
- *User access rights and file permissions.* The concept of "least privileged" is a basic underlying principle for security computer systems and data. It means that users are only granted those access rights and file permissions that they need to do their work. Agencies would benefit from establishing the concept of least privilege as the basis for all user rights and permissions.
- *Network services and devices.* Sensitive programs and information are stored on networks, which are collections of interconnected

[15]Reportable conditions are significant deficiencies in the design or operation of internal control that could adversely affect the entity's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements.

[16]GAO-05-552

computer systems and devices that allow users to share resources. Organizations secure their networks, in part, by installing and configuring networks devices that permit authorized requests and limit services that are available.[17] Agencies need to put in place strong controls that ensure only authorized access to their networks.

- *Audit and monitoring of security-related events.* To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial that agencies implement system or security software that provides an audit trail that they can use to determine the source of a transaction, or to monitor the activities of users on the agencies' systems. To detect and prevent unauthorized activity, agencies should have strong monitoring and auditing capabilities.

Agencies Need to Act to Implement Other Information Security Controls

In addition to electronic access controls, other important controls should be in place to ensure the security and reliability of an agency's data.

- *Software change controls.* Counteracting identified weaknesses in software change controls would help agencies ensure that software was updated correctly and that changes to computer systems were properly approved. Software change controls ensure that only authorized and fully tested software is placed in operation. These controls – which also limit and monitor access to powerful programs and sensitive files associated with computer operations – are important in providing reasonable assurance that access controls are not compromised and that the system will not be impaired. These policies, procedures, and techniques help to ensure that all programs and program modifications are properly authorized, tested, and approved. Failure to implement these controls increases the risk that unauthorized programs or changes could be – inadvertently or deliberately – placed into operation.

[17]Devices used to secure networks include (1) firewalls that prevent unauthorized access to the network; (2) routers that filter and forward data; (3) switches that forward information through segments of a network; and, (4) servers that host applications and data.

- *Segregation of duties.* Agencies have opportunities to implement effective segregation of duties to address the weaknesses identified in this area. Segregation of duties refers to the policies, procedures, and organizational structure that help to ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records. Proper segregation of duties is achieved by dividing responsibilities among two or more individuals or organizational groups. For example, agencies need to segregate duties to ensure that individuals cannot add fictitious users to a system, assign them elevated access privileges, and perform unauthorized activities without detection. Without adequate segregation of duties, there is an increased risk that erroneous or fraudulent transactions can be processed, improper program changes implemented, and computer resources damaged or destroyed.
- *Continuity of operations.* The majority of agencies could benefit from having adequate continuity of operations planning. An organization must take steps to ensure that it is adequately prepared to cope with the loss of operational capabilities due to earthquake, fire, accident, sabotage, or any other disruption. An essential element in preparing for such catastrophes is an up-to-date, detailed, and fully tested continuity of operations plan. To ensure that the plan is complete and fully understood by all key staff, it should be tested, including surprise tests, and test plans and results documented to provide a basis for improvement. Among the aspects of continuity planning that agencies need to address should be: (1) ensuring that plans contain adequate contact information for emergency communications; (2) documenting the location of all vital records for the agencies and methods of updating those records in an emergency; (3) conducting tests, training, or exercises frequently enough to have assurance that the plan would work in an emergency. Losing the capability to process, retrieve, and protect information that is maintained electronically can significantly affect an agency's ability to accomplish its mission.
- *Physical security.* Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed. With inadequate

physical security, there is increased risk that unauthorized individuals could gain access to sensitive computing resources and data and inadvertently or deliberately misuse or destroy them.

In summary, through the continued emphasis of information security by Congress, the administration, agency management, and the accountability community, the federal government has seen improvements in its information security. However, despite the advances shown by increases in key performance measures, progress remains mixed. If information security is to continue to improve, agency management must remain committed to the implementation of FISMA and the information security management program it mandates. Only through the development of strong IT security management can the agencies address the persistent, long-standing weaknesses they face in information security controls.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the Committee may have at this time. Should you have any questions about this testimony, please contact me at (202) 512-6244. I can also be reached by e-mail at wilshuseng@gao.gov. Individuals making key contributions to this testimony include Suzanne Lightman, Assistant Director, Larry Crosland, Joanne Fiorino, and Mary Marshall.

GAO's Mission	The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."
Order by Mail or Phone	The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to: U.S. Government Accountability Office 441 G Street NW, Room LM Washington, D.C. 20548 To order by Phone: Voice: (202) 512-6000 TDD: (202) 512-2537 Fax: (202) 512-6061
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, D.C. 20548
Public Affairs	Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, D.C. 20548

Chairman TOM DAVIS. Thank you.
Ms. Evans.

STATEMENT OF KAREN S. EVANS

Ms. EVANS. Good afternoon, Mr. Chairman. Thank you for inviting me to speak about the status of the Federal Government's efforts to safeguard our information and our systems.

My comments today will focus on the progress we have made in improving the security of the Government's information technology as well as our strategy for addressing continuing security challenges.

This is an extremely important issue for the administration, and it is equally important to me both professionally and personally because some of the government-wide security performance metrics that we use to evaluate the agencies are also included in my personal performance plan.

On March 1st, OMB issued our third annual report to Congress on the implementation of the Federal Information Security Management Act [FISMA]. Much of the information I will be discussing today is provided in more detail in our report. So based on that, sir, I would be happy to answer any questions that you may have about the report and the status and what we are doing going forward.

[The prepared statement of Ms. Evans follows:]

STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

March 16, 2006

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to speak about the status of the Federal government's efforts to safeguard our information and systems.

My remarks today will focus on the progress we have made in improving the security of the government's information technology as well as our strategy for addressing continuing security challenges.

This is an extremely important issue for the Administration. It is equally important to me both professionally and personally because some of the government-wide security performance metrics we use to evaluate the agencies are also part of my personal performance plan.

On March 1st, OMB issued our third annual report to the Congress on implementation of the Federal Information Security Management Act (FISMA). Much of the information I am discussing today is provided in more detail in our report.

Each year, OMB provides to the agencies specific guidance for reporting on the status and progress of their security programs. We use this data to oversee their programs and develop our annual FISMA report. As in the past, this year's guidance included quantitative performance measures for the major provisions of FISMA and for the most part were identical to past years' measures. Consequently, areas of improvement, as well as areas requiring additional management attention are easily discernable.

In addition this year, OMB used the FISMA reporting vehicle to aggregate privacy reporting requirements. The privacy questionnaire -- Section D of the FISMA reporting template -- consolidates reporting under the Privacy Act, the E-Government Act, Section 522 of the Consolidated Appropriations Act and various OMB guidance and policy issuances. OMB's findings and conclusions based on the agencies' privacy reports are contained in OMB's E-Government Report to Congress. OMB will meet with selected agencies over the course of the spring and summer to assist them in enhancing their privacy programs.

Over the past year, Departments and agencies continued to improve their security programs and more fully comply with FISMA. An increasing number of agency systems have received certification and accreditation and annual testing of their security controls. In addition, agency Inspectors General reported improvements in the quality of certification and accreditation and agencies' corrective plans of action and milestones.

Progress in Improving Agency Security Programs

The FY 2005 agency FISMA reports identify progress by individual Departments and agencies in the following areas:

Certification and accreditation of systems

The process for certifying and accrediting information systems is important because it includes assessing risk, developing plans to manage the risk, implementing and testing security controls to ensure they work as intended, and requires an agency manager to verify they understand any residual risk prior to authorizing system operations.

This past year, the number of systems with a formal management approval to operate rose from 77 percent to 85 percent. This improvement is especially notable since the actual number of reported systems increased 19 percent over the last year from 8,623 to 10,289. Several agencies in particular have made outstanding progress: the Department of Defense moved from 58 percent to 82 percent of systems certified and accredited and the Department of Veterans Affairs improved from 14 percent to 100 percent. I am especially encouraged the certification and accreditation percentage for high impact systems is 88 percent -- higher than overall certification and accreditation. This demonstrates agencies are prioritizing their systems and working first to secure the systems presenting the highest risk impact level.

Quality of certification and accreditation processes.

To ensure certification and accreditation achieves the desired outcome, we ask agency Inspectors General (IG) to report on the overall quality of their agency's process. This year, 17 of 25 IGs rated their agency's process as "satisfactory" or better, up from 15 agencies last year.

Quality of agency corrective plans of action and milestone process (POA&M)

OMB also asks IGs to evaluate the effectiveness of agencies' POA&M process for tracking security weaknesses. This year, 19 of 25 IGs rated their agency's process as effective. This is an increase from 18 agencies last year.

Assignment of a risk impact level

FISMA required the National Institute of Standards and Technology (NIST) to develop a number of new standards and guidelines to assist the agencies in securing their

information systems. Among them was a standard for assigning to each agency system one of three security impact levels. The three levels (i.e., high, moderate, or low) reflect the potential impact on organizations or individuals in the event of a breach of security (i.e., a loss of confidentiality, integrity, or availability). Using the impact levels, agencies are better able to prioritize their security needs.

For the first time this year, we asked agencies to report on their implementation of this NIST standard. Agencies have assigned impact levels to 94 percent of the 9,184 systems they manage and 65 percent of the 1,105 systems managed by contractors. For agency managed systems, 18 percent were categorized as high impact, 27 percent as moderate, and 49 percent as low. For contractor managed systems, 27 percent of these were categorized as high impact, 23 percent as medium, and 15 percent as low.

Agency-wide security configuration policy

FISMA requires each agency to develop minimally acceptable system configuration requirements and ensure compliance with them. Standardized configurations reduce system vulnerabilities and simplify security management. All 25 large agencies have an agency-wide security configuration policy in place.

Continuing Challenges

While progress has been made by most agencies, reports continue to identify a number of deficiencies in agency security procedures and practices. Deficiencies are most frequently seen in testing security controls, overseeing contractors, and incident reporting.

Testing of security controls

FISMA requires agencies to periodically test and evaluate information security controls to ensure they are effectively implemented. Although agencies tested security controls on an increasing number of systems (7,425 in FY 2005 as opposed to 6,515 in FY 2004), the overall percentage of systems with tested security controls dropped from 76% to 72%. It should be noted, however, the percentage of high impact systems tested was appreciably higher at 83%.

Oversight of contractor systems

Agency IT security programs apply to all organizations possessing or using Federal information or operating, using or having access to Federal information systems. Therefore, OMB asked IGs to confirm whether the agency ensures oversight of information systems used or operated by a contractor or other organization on behalf of the agency to ensure they met FISMA requirements. Eighteen of 25 IGs said their agency at least frequently performed such oversight. Six IGs said their agency only sometimes or rarely did so. One IG did not report in this area.

Incident Reporting

It is essential for agencies to share information on common vulnerabilities and FISMA requires agencies to report their security incidents to a central incident handling organization. The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) is the designated central incident handling organization and they continue to find sporadic reporting by some agencies and unusually low levels of reporting by others. Less than full reporting hampers the government's ability to know whether an incident is isolated at one agency or is part of a larger event, e.g., the widespread propagation of an Internet worm or an organized attack by an adversary.

How Do We Oversee Agency Performance?

OMB will continue to use the oversight mechanisms described below to improve agency and government-wide IT security performance.

President's Management Agenda Scorecard

In addition to annual reporting by the agencies, the President's Management Agenda (PMA) Expanding Electronic Government (E-Government) Scorecard includes quarterly reporting on efforts to meet their security goals. Agencies must provide OMB with a quarterly update on IT security performance measures and POA&M progress. The quarterly updates enable the agency and OMB to monitor agency remediation efforts and identify progress and problems.

The updates are used to rate agency progress and status as either green (agency meets all the standards for success), yellow (agency has achieved intermediate levels of performance in all the criteria), or red (agencies have any one of a number of serious flaws).

Information technology security is one of a number of critical components agencies must implement to get to green (or yellow) for the E-Government scorecard. If the security criteria are not successfully met, agencies cannot improve their status on the scorecard. Agencies are publicly accountable for meeting the government-wide goals, and scores are posted quarterly at http://results.gov/agenda/scorecard.html

To "get to green" under the Expanding E-Government Scorecard, agencies must meet the following three security criteria:

- Inspector General verifies the effectiveness of the Department-wide IT security remediation process;
- Inspector General rates the agency certification and accreditation process as "Satisfactory" or better; and
- The agency has 90 percent of all IT systems properly secured (certified and accredited).

In order to "maintain green," by July 1, 2006, agencies must have:

- All systems certified and accredited;
- Systems installed and maintained in accordance with security configurations; and
- Consolidated and/or optimized all agency infrastructure to include providing for continuity of operations.

OMB will continue to use the E-Government scorecard to motivate agency managers and highlight areas for improvement.

Review of Agency Information Technology Investment Requests

Several years ago, OMB integrated information technology security into the capital planning and investment control process to ensure security was built into and funded over the lifecycle of each agency system. This also helps promote greater management attention to security as a fundamental priority. To guide agency resource decisions and assist oversight, OMB's policies require agencies to:

- Report security costs for all information technology investments;
- Document that adequate security controls and costs have been incorporated into the life cycle planning of each investment; and
- Tie the POA&Ms for a system directly to the funding request for the system.

Additionally, agencies must answer a series of security questions and describe how the investment meets the requirements of the FISMA, OMB policy, and NIST guidelines. The justifications are then evaluated on specific criteria including whether the system's cyber-security, planned or in place, is appropriate.

Information System Security Line of Business (ISSLOB)

Over this past year, an inter-agency task force identified common solutions to be shared across government and developed a draft joint business case outlining a general concept of operations with overall milestones and budget estimates. The Task Force identified common solutions in four areas – training, reporting, incident response, and evaluating and selecting security products and services. All agencies were asked to submit proposals to either become a service provider (Center of Excellence) for other agencies, or migrate to another agency from which they would acquire expert security services. The Department of Homeland Security is continuing to serve as the program manager for this effort and will work with those agencies proposing to become centers of excellence to bring greater clarity to their proposals. OMB intends to use the ISSLOB to achieve greater efficiency and effectiveness through standardizing and sharing capabilities, skills, and processes across government, to the maximum extent practicable.

Conclusion

Over the past year, agencies made steady progress in closing the Federal government's information technology security performance gaps. Analysis of baseline performance measures indicates policy compliance improvements in a number of programs. However, inconsistent implementation of security measures across the Federal government leaves weaknesses to be corrected. OMB encourages CIOs and IGs to work together to remediate these deficiencies.

As part of its oversight role, OMB will use quarterly reporting mechanisms to track key performance metrics for FISMA compliance. Agency status and progress will be reflected on the President's Management Agenda scorecard.

Finally, the Administration intends to focus on the implementation of an information security line of business to reduce costs and increase security effectiveness across government. The establishment of Centers of Excellence for security training and FISMA reporting will be a first step towards ensuring greater use of standardized products and services.

Chairman TOM DAVIS. Ms. Evans, let me start with you. Do you plan to issue new or updated guidance regarding your Circular A–130?

Ms. EVANS. We do not plan to issue updated guidance on A–130 because we believe that it is based on sound principles that are already reflected in FISMA. With NIST issuing new standards and guidance, we really don't think that we need to revise A–130 at this time, but we will continue to review it.

Chairman TOM DAVIS. All right. In this year's report, just like last year's report, you mentioned that reporting to US-CERT is sporadic and not complete. What steps are you and US-CERT taking to ensure that agencies are more compliant in these incidents?

Ms. EVANS. In May 2005, we did issue a reporting concept of operations out to the agencies, and so what OMB and DHS are planning to do is followup specifically with the agencies that did not report any incidences to US-CERT to make sure that we all are operating from the same understanding so that we can go back and double-check that an incident is an incident based on this concept of operations that was approved by all the agencies as well.

Chairman TOM DAVIS. Now, although there has been improvement, there are still several agencies that don't have complete inventories. These include some of the largest: DOD, USDA, Treasury, HHS, and VA.

You know, without accurate inventories, how can you be sure that the agencies are making progress? And while C&As are an important component of security, knowing what systems you are running is even more essential. Have you emphasized or has OMB emphasized to the agencies the necessity of a complete inventory? And what challenges have they reported to you in trying to create and maintain an accurate inventory?

Ms. EVANS. Yes, sir, we have worked with the agencies, and in the places where the agencies haven't had a completed inventory based on what the IGs have reported, we are meeting specifically with those agencies to be able to address what issues are keeping them from meeting the inventory. But, also, we have included this in the President's management agenda as one of the criteria and that we do assess the agencies on a quarterly basis of their progress on performance.

So once an agency makes green, in order to maintain green they have to have a completed inventory.

Chairman TOM DAVIS. Thank you. Identity theft continues to be a growing problem, especially with the loss of personal and sensitive information. Data breach laws at the State level which require companies to inform individuals when the organization suffers a breach that exposes their personal information have improved our understanding of this problem. Congress is considering a national data breach notification standard. Currently, there is no requirement for Federal agencies to notify citizens in case there is a breach. I have a few questions along those lines.

One, do Federal agencies notify citizens when a breach of personally identifiable information occurs on Government data bases?

Ms. EVANS. In responding to that question, sir, we believe the Privacy Act has provisions that address this. But what I would like to do is be able to go back and do a more in-depth analysis and

be able to take this question for the record and give you a more thoughtful response about how we should be responding to this.

Chairman TOM DAVIS. I appreciate that, because that is something that comes up time and time again.

What, if any, guidelines exist to determine if a breach requires notification?

Ms. EVANS. Again, sir, I need to go back and further research this based on what we have put in place with the Privacy Act, and I would like to take this question for the record so that I can give you a more thoughtful response.

Chairman TOM DAVIS. Let me ask you something on RFID technology, radiofrequency. RFID technology is being implemented by DOD for tracking supplies. It is being implemented by the State Department for immigration documents and passports. Other agencies may choose to use the technology to control access to physical and logical assets to comply with Homeland Security Presidential Directive 12. A May 2005 GAO report on the Federal Government's use of RFID highlighted FISMA security practices in the context of security concerns with RFID technologies.

What agencies within the Federal Government are using RFID technologies for applications that involve sensitive personal information?

Ms. EVANS. You have mentioned the State Department, Department of Defense, DHS. What we would like to do is go back and look more completely at each of the agencies to see what their plans are as it relates to the deployment of RFID beyond what we already have planned.

Chairman TOM DAVIS. Do you think there is a need for a national standard for maintaining the security and privacy of personal information collected using RFID technology?

Ms. EVANS. We believe that if you currently implement the security policies and practices that are in place, if you implement them adequately, those practices and policies would be able to protect the information regardless of the technology, whether it was RFID or any other new emerging technology that would come out.

Chairman TOM DAVIS. So how do you fine-tune FISMA regarding the use of RFID technology given its increased adoption by Federal agencies that are required to meet FISMA standards?

Ms. EVANS. Well, I would recommend at this point that FISMA is about good security practices. It is about managing the risk associated with your security program and your information technology and assets. And it is really not specifically about technologies but about our ability to manage those technologies as we implement them.

So in conjunction with working with NIST and having NIST issue policies, guidelines, the standards that they do, I think FISMA is adequate the way that it is, and it is up to us and then the agencies to manage that risk as new technologies come out.

Chairman TOM DAVIS. OK. Mr. Wilshusen, let me just ask, it seems that when we look over the grades, the largest agencies or those agencies with diverse missions seem to be at the bottom of the grading while the smaller of the major agencies or those with single, well-defined missions seem to improve their grades. How do

you think the diverse mission and size play into the issue of information security?

Mr. WILSHUSEN. Well, I think certainly that size and the complexity of the organization influences the way an organization organizes, manages, and secures its information technologies. Large Federal departments have multiple, sometimes semi-autonomous operating bureaus and divisions that may have separate missions, business processes, cultures, and technologies that support those processes.

However, at some level those technologies interconnect with other systems and networks with other bureaus, and consequently, there might be vulnerabilities in one particular agency or bureau that has an impact on others. Thus, there is really a need for strong security management over that area. However, because these bureaus may be somewhat semi-autonomous and have separate funding, they may not necessarily be conducive to implementing or ceding some of their authority for securing these systems.

It is going to take—and the departments might have a more challenging role in trying to create and develop and implement an agency-wide information security program. It is going to require that agency top management and the management of the different bureaus be held accountable and support and be committed to implementing an agency-wide information security program.

Chairman TOM DAVIS. I think there is a perception in some circles, it seems to me, that FISMA is largely a paperwork exercise. What is your reaction to that?

Mr. WILSHUSEN. FISMA is designed to be a comprehensive framework for ensuring the effectiveness of information security controls over the information resources that support Federal operations and assets. It requires Federal agencies to develop, document, and implement an agency-wide information security program that contains various elements. Each of these elements is based on best industry practices. These include assessing the risk, developing risk-based policies and procedures that cost-effectively reduce those risks to an acceptable level. It also requires that agencies provide the training to their employees and contractors to inform them of what these risks are and their responsibilities for practicing and implementing strong security throughout the organizations.

It also requires that agencies test and evaluate the effectiveness of their controls over their systems on a periodic basis, and if there are problems, if there are weaknesses, to take corrective actions.

These are just basic information security principles and practices that should be implemented. If agencies are reducing FISMA implementation to a paperwork exercise, then they are not going to enjoy the benefits offered by implementing them.

Chairman TOM DAVIS. Can you think of any incentives or penalties that should be added to improve the agency scorecard ratings?

Mr. WILSHUSEN. One might be looking at the funding. I believe at one point in time there was discussion on whether agencies, you know, should be looking at the funding, should they be adjusted, should—for agencies that do well versus those that do not.

Chairman TOM DAVIS. How about the——

Mr. WILSHUSEN. But that is a double-edged sword.

Chairman TOM DAVIS. Of course it is. You are taking money from the people who need it the most.

Ms. Evans, do you have any thought on that?

Ms. EVANS. When we do the analysis for the President's budget every year, one of the key priorities is the cyber security program of each of the agencies. So we do continue to put a priority on that and make sure that agencies that don't have a good security program, that the priority for the funding going forward is spent on that first and that—and we have broken out the budget this year when we submitted the 2007 budget, broke out and showed the relationship of their overall IT budget to the percentage that they spend on IT security as well, and continue to put the priority on that.

The thought from the administration is that you should not layer new things on top of bad things. And so you need to fix the cyber security aspects of that based on all the issues that you brought up already today about implementing new technologies and those types of things.

So the incentive is the more efficient you are at getting it done, not just generating the paperwork but really fixing the security and mitigating the risk, then you can move forward and use the funds that you had planned to use for those new activities within your agency or department.

Chairman TOM DAVIS. And you think the budget reflects that to some extent, is what you are saying?

Ms. EVANS. Yes, sir. Yes, sir.

Chairman TOM DAVIS. Ms. Watson.

Ms. WATSON. I missed most of the testimony. I want to thank the chair for having this hearing. But what stands in our way from preventing the hacking and the taking of information and putting illegal information into the process in our computers? What stands in our way from stopping that?

Mr. WILSHUSEN. One is making sure that the agencies have fully implemented an information security program within that particular agency.

Ms. WATSON. Why haven't they?

Mr. WILSHUSEN. Well, that is a good question and that is one that we constantly seek the answer to. In our reviews we look, when we conduct an information security audit at the Federal agencies, we look at the type of controls that they have in place, the effectiveness of those controls, and we have often found that numerous vulnerabilities exist within their access controls that are designed to prevent limit and detect access to their information resources. We also find other types of general controls related to their physical security over their computing resources that also could lead to the unauthorized disclosure, deletion, alteration of sensitive information. And these types of weaknesses have been identified at numerous agencies that we have done audits at.

Ms. WATSON. Well, is it that we don't have the technology knowledge to do something? I mean, I know you are auditing, you are looking. Is it lack of technology knowledge? Is it lack of setting a priority? Is it lack of the funding? Did you—where would you put your finger, if we were to correct this and do it in a hurry? Because

I flip on CNN or I flip on one of the morning programs and I find that in our Federal computers people have pornography, etc. How does that happen?

Mr. WILSHUSEN. Well, certainly there are technical controls that need to be improved and in place to help protect that from happening. But first and foremost, we see information security as a management issue and that it receives sufficient attention and implementation throughout the organization, from top-level management through all layers of the organization, because each and every person has responsibility for information security. But in terms of the management, we do look at various different aspects in terms of is the organization assessing the risk accordingly for the type of information that it collects and processes and maintains; are they developing those policies and controls that are needed to protect that information?

And what we often find is, yes, they do that to an extent, and they may develop policies and procedures that are designed, at least, to protect the information and implement strong controls, but a lot of times they are not implementing it. And this often occurs even though at the department level they might have strong policies——

Ms. WATSON. Well, let me just stop you there. Does it go to incompetence? You know, I am reading here, each agency is also required to do an annual independent evaluation—let's say of information security. Why would it not be done? And why could they not address it?

You know, we are the policymakers here. You are in front of this committee. Maybe you can give us some idea of what our next piece of legislation needs to be.

Mr. WILSHUSEN. I would like to answer the first question you had there first.

Ms. WATSON. OK.

Mr. WILSHUSEN. Certainly one of the reasons why there continue to be information security weaknesses at the organizations that we audit is that it is a complex and challenging job. Many of these computing environments, particularly at the larger agencies, have highly complex distributive information systems and networks that are, because of their interconnectivity, vulnerabilities that exist on one server can affect an entire network. And some of these agencies have thousands of servers. And so it is a very dynamic environment in which new applications, new servers, new technologies are being implemented. And if the agencies are not effectively assessing their risk and monitoring the implementation of these technologies on a regular basis, vulnerabilities crop up. And that is how hackers, that is how individuals within the organization can exploit those vulnerabilities for either personal or—gain.

Ms. WATSON. I heard the key words: effectively assessing.

Mr. WILSHUSEN. Yes.

Ms. WATSON. And, you know, we ought to be looking at systems before we contract and bring them in to see if they would fit in. Otherwise—you know, we need to plan and we need to assess and evaluate that plan, and we need to have a report. I think that is a requirement. And certainly, you know, new technology adds to

the complexities of these systems, but we have to have an overall plan, a master plan.

Mr. WILSHUSEN. Right. And that is one of the benefits of FISMA, of what it provides, is that it requires that agencies implement an agency-wide information security program, and that includes addressing security throughout the entire life cycle of any new technologies or its applications or systems that are being introduced into the department.

Ms. WATSON. Thank you very much. Appreciate it.

Chairman TOM DAVIS. Mr. Clay.

Mr. CLAY. Thank you, Mr. Chairman.

For Mr. Wilshusen, GAO recently completed a draft report for me on the impact the National Information Assurance Partnership program is having on information security within classified programs. Can you speak to the merits of extending NIAP product validation out to those agencies in the non-national security community?

Mr. WILSHUSEN. Sure. All these results are—as you mentioned, we do have a draft report out. It is presently out for comment with the DOD and the agencies. We have not yet received their comment. We anticipate issuing that report later this month in final.

But let me just at least talk about the observations that we have identified so far with that program. We identified that the NIAP program does indeed provide and offer some benefits. One, it provides another set of eyes and ears to look and test the security features of information security or systems products that an agency is considering procuring. It also, through the evaluation process, has identified and uncovered flaws within those products. And what we have found and based on our interviews with vendors, the participants in the program, is that the vendor is often correct in those flaws that are identified.

And another benefit is that, after going through these processes, some of the vendors decided that they—actually changed their development processes to accommodate the new strength and to mitigate any weaknesses that were identified as their products were evaluated.

But at the same time, there are still a number of challenges associated with that program. These also include that, for one, the product is not evaluated against a set of particular requirements. It is more looked at the—it is evaluated based on the procedures that are used to develop the product. Another vulnerability is—or I should say another challenge deals with the cost and time that is involved in processing and evaluating these products. We have found that vendors thought it was too costly and took a long period of time to do so.

Some of the agencies felt that they did not have a really full population or a pool of evaluated products to choose from. Sometimes, because of the length of the evaluation process, new versions of the product under evaluation were being issued, so they couldn't necessarily get the latest and greatest version of the product.

So there are a couple of challenges associated with that program.

Mr. CLAY. On finding the weaknesses and coming back and correcting it, who gets the bill for that? Do the vendors eat the cost, or do the taxpayers pay the cost?

Mr. WILSHUSEN. I don't know if I can answer that. It is up to the vendors. It depends on, I guess, the contractual requirements, but it is up to the vendors to take the corrective actions on that. Whether they subsequently pass the costs along to the procurers of the product, I can't answer that.

Mr. CLAY. Thank you. Thank you for your response.

Ms. Evans, perhaps you may be able to shed some light on that. But let me ask you, you know, the number of annual risk assessments conducted last year declined when compared to fiscal year 2004 even though the number of systems online increased by nearly 20 percent. DHS—first, what were the factors contributing to this problem at first? Talk to me about DHS, which once again—well, go ahead.

Ms. EVANS. Well, as you stated, the risk assessments did go down, but we did get an increase in the number of systems that are out there. However, this is also the first year where we did ask the agencies to also assess the systems that they had based on impact, like high, medium, and low impact of those systems. And the agencies did focus their risk assessments on the high-impact systems. And 88 percent of those, I believe, were the ones where the risk assessments going forward on that.

So we did ask them to make sure that their priority was done the high-impact systems as they were doing the risk assessments, going through and doing the certifications and accreditations, because that is one piece of the certification and accreditation that the agencies do.

Mr. CLAY. OK, let me stop you there since——

Ms. EVANS. Sure.

Mr. CLAY. Real quickly, give me your impression of ineptitude at DHS in this whole arena. Talk to me about that, as far as them being the coordinator of key information-sharing responsibilities, or a legacy system, are the 22 agencies proving to be too difficult to bring into compliance, or are there other factors?

Ms. EVANS. Well, DHS is a challenging environment. By bringing all the departments and agencies together there, this really does exemplify the complexity of an environment of a large department that would have to be managed to make sure that you have a good program in place. So what DHS is doing is moving forward trying to bring all that management in place to ensure that they have a good cyber security program and that they can move forward and protect that information and those assets.

It does take some time to really be able to demonstrate that progress. And I would say that the things that DHS is doing we may not necessarily see in all the metrics as we measure them in FISMA. But you have brought up that the independent audit is also an essential piece so that they can feed back the results of that from their IG into their programming, to make sure that they are improving that as they go forward.

Mr. CLAY. Yes. Thank you, but it sounds as though you are defending the incompetence of DHS. Thank you.

Chairman TOM DAVIS. Anything else you want to add?

We will dismiss this panel, take a 2 minute recess, and we will come to the next one.

Thank you all very much.

[Recess.]

Chairman TOM DAVIS. Thank you all for your patience.

We are going to now recognize our second distinguished panel. We have Mr. Thomas P. Hughes, Chief Information Officer, U.S. Social Security Administration; we have Mr. Thomas Wiesner, the Deputy Chief Information Officer, U.S. Department of Labor; Mr. Robert Lentz, Information Assurance Director at the U.S. Department of Defense; and Mr. Scott Charbo, the Chief Information Officer at the U.S. Department of Homeland Security.

It is our policy we swear you in before your testimony, so if you would just rise and raise your right hands.

[Witnesses sworn.]

Chairman TOM DAVIS. Thank you very much.

Well, you know our rules. We try to hold to 5 minutes. Your entire statement is in the record. We very much appreciate your being with us today. I apologize for the delay with the floor votes, but I think we will be able to move ahead fairly expeditiously here, uninterrupted.

Mr. Hughes, we will start with you and we will work straight on down the line. Thank you again for being with us.

STATEMENTS OF THOMAS P. HUGHES, CHIEF INFORMATION OFFICER, U.S. SOCIAL SECURITY ADMINISTRATION; THOMAS WIESNER, DEPUTY CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF LABOR; ROBERT F. LENTZ, DIRECTOR, INFORMATION ASSURANCE; U.S. DEPARTMENT OF DEFENSE; AND SCOTT CHARBO, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF THOMAS HUGHES

Mr. HUGHES. Chairman Davis and members of the committee, thank you for inviting me here today to discuss information security at the Social Security Administration. As Chief Information Officer for the agency, I appreciate the opportunity to discuss our implementation of FISMA, the Federal Information Security Management Act of 2002, and our agency's accomplishments in securing and protecting the information in the records we maintain.

SSA has always recognized the importance of protecting the security and privacy of the people we serve and ensuring the integrity and accuracy of the records we maintain. The Social Security Board's first regulation, published in 1937, dealt with confidentiality of records. For more than 70 years we have honored our commitment to the American people to maintain the confidentiality of these records. This longstanding emphasis on privacy has led to a strong commitment in information security.

While we have always safeguarded our records, we also work continuously to ensure that our information technology programs remain responsive to evolving conditions, and we use a variety of proactive security measures, plus independent testing and evaluation security controls, to protect these records. We take an agency-wide approach to information technology security at SSA. SSA's deputy commissioners, along with the CIO, are accountable for the certification of our major IT systems and help to ensure that our IT assets are adequately secured.

Here are some of the major highlights of our FISMA 2005 report: All 20 of SSA's major IT systems were certified and accredited.

SSA had incorporated National Institute of Standards and Technology security controls into our System Development Life Cycle process.

SSA provided IT security awareness to all of our employees, including contractors, and gave specialized in-depth training for those with significant IT security responsibilities.

The Office of Inspector General's independent evaluation of our information security program for 2005 confirmed that SSA's remediation, certification and accreditation, and inventory processes are sound. The OIG made a number of recommendations for improvement that we are implementing.

For instance, first, we developed security documents for every enterprise architecture platform in the agency and expanded this initiative into the data base environment as well. In addition, we implemented a monitoring program for each system configuration standard and risk model.

Second, we agreed with the IG recommendation that SSA should regularly update our continuity of operations plan [COOP], with a disaster recovery plan. SSA also has and will participate in disaster recovery exercises, which help validate key elements of our COOP.

Finally, to respond to the recommendation regarding improving how we monitor contract security awareness training, we are implementing a process where all contractors with systems access will complete a security awareness training module that will allow us to monitor the process.

You asked us to describe the way SSA identifies and tracks information technology security weaknesses. The answer is that SSA is using an automated software tool that allows us to follow corrective security actions all the way to completion. In addition, the system generates detailed reports which then allow management to better evaluate the security status of their systems.

You also asked about guidance—resources and/or procedures agencies need to comply with FISMA. I believe that agencies need to constantly challenge the traditional status quo if we are to maintain and enhance our security procedures and comply with FISMA. This is critical in any security environment, but particularly important in today's challenging information environment.

While we are proud of our accomplishments, Commissioner Barnhart and all of us at SSA recognize that we must be vigilant in every way to assure that the personal information SSA collects remains secure, the taxpayer dollars are protected, and that public confidence in the Social Security system is maintained.

Mr. Chairman, thank you for the opportunity to speak before this committee. I will be pleased to answer any questions.

[The prepared statement of Mr. Hughes follows:]

Government Information Security and Implementation of FISMA

Statement of

Thomas P. Hughes
Chief Information Officer
of the
Social Security Administration

Before the
Committee on Government Reform

March 16, 2006

Statement of Thomas P. Hughes
Chief Information Officer
of the
Social Security Administration
Before the
Committee on Government Reform
March 16, 2006

Mr. Chairman and Members of the Committee, thank you for inviting me here today to discuss government information security at the Social Security Administration (SSA). Commissioner Barnhart, the executives at the agency and I place the highest importance on our information security program and are committed to securing and protecting Federal information. As SSA's Chief Information Officer (CIO), I appreciate the opportunity to discuss our implementation of the Federal Information Security Management Act of 2002 (FISMA).

SSA recognizes the importance of protecting the security and privacy of the people we serve and ensuring the integrity and accuracy of the records we maintain. The Social Security Board's first regulation, published in 1937, dealt with the confidentiality of SSA records. For more than 70 years, since long before the advent of computers and the technology age, SSA has honored its commitment to the American people in maintaining the confidentiality of our records. Our emphasis on privacy has led to a strong commitment in information security.

While we have always safeguarded our records, we also work continuously to ensure that our information technology programs remain responsive to evolving advancements, conditions, and security vulnerabilities. SSA uses a variety of proactive security measures plus independent testing and evaluation of security controls to protect the information that the American public entrusts with us.

Today, as I discuss SSA's compliance with FISMA, and the areas in which we have made significant improvements as well as the areas in which we strive to improve, I am confident you will understand the care I must take in any discussion of the technical details of our specific security processes in a public forum.

Background on FISMA at SSA

The E-Government Act (Public Law 107-347) passed by the 107th Congress and signed into law by the President in December 2002 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, or FISMA, requires each Federal agency head to be responsible for security issues including:

- Providing information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information collected or maintained by or on behalf of the agency
- Complying with the requirements of FISMA and related policies, procedures, standards and guidelines
- Ensuring that information security management processes are integrated with agency strategic and operational planning processes
- Ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control
- Delegating to the agency Chief Information Officer (CIO) the authority to ensure compliance with FISMA including the development of an agency-wide information security program
- Reporting annually to Congress the adequacy and effectiveness of the information security policies, procedures and practices as well as compliance with FISMA

FISMA, along with the Clinger-Cohen Act of 1996 and the Paperwork Reduction Act of 1995, explicitly emphasizes a risk-based policy for cost-effective security. In support of and reinforcing this legislation, the Office of Management and Budget (OMB), through Appendix III of Circular A-130, requires executive agencies within the federal government to:

- Plan for security;
- Ensure that appropriate officials are assigned security responsibility;
- Periodically review the security controls in their information systems; and
- Authorize system processing prior to operations and, periodically, thereafter.

The ultimate objective is to conduct the day-to-day operations of the agency and to accomplish the agency's stated missions with adequate security, or security commensurate with risk, including consideration of the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

SSA takes its responsibility in meeting the requirements of FISMA very seriously. As the Chief Information Officer, I am directly responsible to the Commissioner for ensuring under FISMA that the IT resources of the Agency are adequately secured. The FISMA Certification and Accreditation (C&A) processes provide me, as CIO, and other senior agency officials, with a current picture on the security status of SSA's 20 major IT systems. All of these systems are important to the performance of our mission. These information systems allow us to run disability processes, recover overpayments, maintain audit trails, track our human resources, and maintain numerous information databases.

We take an agency-wide approach to information technology security at SSA. The CIO and the agency's Deputy Commissioners for Operations, Disability Income Security Programs, Systems, Human Resources, and Finance, Assessment and Management share the accountability for the FISMA C&A process for the major IT systems. In addition, the OCIO works collaboratively with all agency level organizations to ensure that our IT assets are adequately secured.

FISMA Compliance at SSA

SSA uses the FISMA reporting process as an important indicator of how the agency's information technology assets and resources are being protected. Here are the major highlights of the agency's report for FY 05:
Major Systems: SSA has a total of 20 Agency Major Information Systems. All 20 of these systems are currently certified and accredited. In addition, SSA's contingency plan and security controls were tested for each system in the past year.

NIST Security Standards and Guidance: Under FISMA, OMB and the National Institute of Standards and Technology (NIST) develop guidance and standards for Agency systems and security programs. NIST security controls are incorporated into our System Development Life Cycle process. SSA uses special automated software tools to support security self-assessments required by FISMA. These tools also allow us to track any security weaknesses identified.

Incident Detection: SSA follows documented policies and procedures for identifying and reporting incidents of security weakness and uses a combination of automated tools, system monitoring tools and network-penetration type reviews to protect all 20 of our information systems. As required by NIST, SSA provides monthly incident reports to the US Computer Emergency Readiness Team.

Training: SSA provided IT security awareness training to all of our employees (including contractors) and specialized in depth training for those with significant IT security responsibilities. Contractors are required to possess security credentials, expertise and training appropriate to the functions they will be performing before they are permitted to perform services under a contract.

Configuration Management: SSA has an agency wide security configuration policy which is updated as needed to reflect changes in computing platform and in security configuration. All of the operating systems software used at SSA (Windows, Solaris and UNIX, HP, etc) have security configuration policies implemented.

SSA submitted its report for FY 2005 to OMB on October 7, 2005. In March of 2006, OMB provided a combined Federal Agencies FISMA Report which was submitted to Congress.

SSA Office of Inspector General (OIG) FISMA Report

In the second part of the agency's annual FISMA report to OMB, SSA's OIG independently evaluates SSA's information security program and practices. In the FY 2005 report, the OIG determined that SSA met the requirements of FISMA, pointing out that "SSA continues to work towards maintaining a secure environment for its information and systems and has made improvements over the past year to further strengthen its compliance with FISMA". The OIG confirmed that SSA's remediation, certification and accreditation, and inventory processes are sound and made a number of recommendations for improvement:

- *Fully comply with the Agency's risk models and configuration guides.* In response to the recommendation to fully comply with risk models and configuration guides, SSA has developed security documents for every Enterprise Architecture platform in the Agency and expanded this initiative into the database environment as well. We have also developed a cyclical update process for all risk models and configuration guides. We strive to evaluate our architecture for documented mitigations against the latest risks.

  Equally important, the Agency has implemented a monitoring program for each system configuration standard and risk model. This monitoring program provides an accurate and quantifiable picture of the current compliance levels and helps us to meet our FISMA reporting requirements.

- Ensure that the Continuity of Operations Plan (COOP) is updated and tested appropriately. We agree that SSA needs to make sure that both COOP and the Disaster Recovery Plan are updated regularly so that SSA can function in the event of an emergency or disaster. SSA has a schedule for the annual review and update of the COOP plans at the Agency and component levels. The review and update process is conducted in cycles, with the result that updating and testing of the SSA COOP happens on a continuing basis.

  In addition, SSA participated in "exercise Pinnacle," the government-wide COOP exercise last year. This summer, we will participate in "Forward Challenge 06". These exercises validate key elements of the SSA COOP Plan.

  As noted in the OIG's report, the Disaster Recovery Exercise (DRE) was postponed with the concurrence of the OIG and its auditors. The Agency completed its DRE exercise in January 2006. The 2 week exercise was

expanded to include more systems and computing platforms along with additional contractors involved with the testing effort.

- *Improve monitoring of contractor security awareness training.* To respond to this recommendation, SSA is implementing a process where all contractors with systems access will complete a security awareness training module. This module provides direct links to current security awareness policy documents as the trainee goes through the program. The trainee is given positive reinforcement through automated responses to answers in the module. The module also allows the agency to monitor the training process and gives an accurate total of trainees who have taken the module.

Other Issues

In the letter of invitation from the Committee, SSA was asked to describe how the Agency identifies and tracks information technology security weaknesses. SSA has established a formal process to track, monitor and resolve weaknesses identified through the FISMA reporting process. SSA is using an automated software tool that allows us to follow corrective security actions through to completion. In addition, the tool produces reports which then allow management to better evaluate the security status of their systems. Other Federal agencies, such as the Environmental Protection Agency, are also using this tool to track, monitor and resolve IT security weaknesses.

The Committee also asked about guidance, resources, and / or procedures agencies need to comply with FISMA. I believe that agencies need to constantly challenge the traditional 'status quo'. This is critical in any security environment. To be responsive to evolving advancements, conditions, and vulnerabilities, agencies must acknowledge the requirement to continue to improve systems information security on a day-to-day basis. Leadership is also very important. Agencies must have leaders that truly understand today's security challenges and have the vision to imagine challenges of the future.

Conclusion

Mr. Chairman, Commissioner Barnhart and I, along with all of the senior executives at the Social Security Administration, recognize that information technology systems security is an ongoing challenge and critical component of our mission. While we plan on further improvements with our FISMA reporting in the coming year, we also recognize that FISMA compliance is just one mechanism for security analysis and reporting. Additional and regular internal information technology security evaluations and improvements are also critical pieces to further maintain effective security. We must be vigilant in every way to assure that an individual's personal information remains secure, taxpayer dollars are protected, and that public confidence in Social Security is maintained. We look forward to working with the Committee to assure the American people that we are doing all we can to maintain the security of the information entrusted to

us. Thank you for the opportunity to speak before this committee and I am happy to answer any questions.

Chairman TOM DAVIS. Mr. Hughes, thank you.
Mr. Wiesner, thanks for being with us.

STATEMENT OF THOMAS WIESNER

Mr. WIESNER. Good afternoon, Chairman Davis and members of the committee. Thank you for inviting me here today to discuss the Department of Labor's implementation of the Federal Information Security Management Act and the lessons learned over the past several years.

Today I will first speak on the challenges the Department has faced over the last few years in implementing its computer security program. I will then expand on the current status of our program and highlight many of the significant improvements. Last, I will provide a snapshot of opportunities for improvement and labor strategy to address those areas.

Labor's organizational components, including the Office of the CIO, had different viewpoints FISMA compliance. Additionally, we were an organization of distinct agencies that in many cases operated independently and accomplished individual goals through various IT solutions. Labor agencies, the OIG, and the Office of the CIO were all focused on different and sometimes conflicting priorities. We had to change this culture, including attention to IT security as a key part of everyday business. Under the CIO's direction, the Department arrived at a consensus and we have moved forward to ensure our compliance with FISMA.

To that end, the following actions were carried out: In 2001, a security manager was hired and placed in the Office of the CIO to manage the Department-wide security program.

In 2002, our IT security policies and procedures were updated to incorporate current OMB and NIST guidance.

In 2003, the Department established a Technical Review Board IT Committee subcommittee comprised of agency security managers. This board serves as the Department's first tier of investment review for major IT investments and as a forum to identify and resolve Department-wide IT-related issues, including computer security.

In 2003, Secretary Elaine Chao institutionalized a culture of policy and strong computer security under a Secretary's order issued in May 2003. This order outlines the roles and responsibilities for managing information technology at the Department, to include IT security responsibilities.

In 2003, the Department developed an eGovernment Strategic Plan that ties IT security to the Department's mission.

In 2005, the Department updated its IT Strategic Plan, where IT security goals and direction were incorporated.

At Labor our computer security program has progressed from a grade of F in 2001 to a B- in 2004. Additionally, our computer security program was a significant contributor to the Department's achieving and maintaining a "Green" rating on Expanded Electronic Government on the President's management agenda scorecard.

The successes we have achieved to date can be attributed to strong oversight of Department-wide security issues, cooperation at the IT senior management level, and continuous collaboration

through Department-wide reviews. The efforts of the Labor IT Security Subcommittee results in sound security practices that enable consistent FISMA reporting from the CIO and the OIG. This is attributed to the following successes: A fully integrated computer security program with capital planning and enterprise architecture programs. A revised system development life cycle management manual to include security requirements at each phase. An OIG-approved plan of action and milestones program since 2003. Quarterly capital planning program reviews that ensures adequate IT security expenditures and semiannual eGovernment reviews of all DOL agencies modeled on the PMA scorecard and FISMA performance metrics.

Correspondingly, the Department has maintained a comprehensive Certification and Accreditation program, achieving authority to operate for 100 percent of our major information systems, up from 97 percent in fiscal year 2004.

Despite this progress in securing our IT systems at DOL, we recognize that security is a constant challenge and a task that can never be considered complete. We have identified three areas for strengthening our computer security program: general and application security controls, patch management, and IT security manager skill competencies.

The Department has developed a comprehensive work plan to address these issues, to include the implementation of NIST 800–53 and a Certified Information Systems Security Professional training program and certification exam for DOL security managers.

In conclusion, computer security is a core element of our business and culture at the Department of Labor. Secretary Chao, Deputy Secretary Law, agency senior management, and the dedicated DOL IT professionals are committed to the Department's computer security program. As we face the evolution of FISMA compliance, we will strive to maintain a balance of FISMA reporting requirements and the implementation of sound security practices.

Mr. Chairman, thank you for the opportunity to provide this brief outline. I would be happy to answer any questions. Thank you.

[The prepared statement of Mr. Wiesner follows:]

Statement of Thomas Wiesner
Deputy Chief Information Officer
U.S. Department of Labor
Before the U.S. House of Representatives
Committee on Government Reform

March 16, 2006

Good afternoon, Chairman Davis and Members of the Committee. Thank you for inviting me here today to discuss the Department of Labor's (DOL) implementation of the Federal Information Security Management Act (FISMA) and the lessons learned over the past several years of our Computer Security Program. But first, let me state that we at the Department of Labor congratulate you on your Committee's efforts to improve the computer security for the Federal Government. Your attention to this important issue keeps us focused and we understand that the Federal Government still has a way to go to achieve the strong computer security posture needed to adequately protect our information and systems. You have our assurance that DOL will do its part.

Today I will first speak on the challenges the Department has faced over the last few years in implementing its Computer Security Program. I will then expand on the current status of the Department's security program and highlight many of our significant improvements. Lastly, I will provide a snapshot of opportunities for improvement and DOL's strategy to address those areas.

Challenges

1. Establishing a coherent perspective of FISMA

   For a host of reasons, DOL organizational components, including the Office of the Chief Information Officer (OCIO), had different viewpoints on compliance with FISMA. Under my direction, the Department ultimately arrived at a consensus, and we have moved forward to ensure our compliance with FISMA.

2. Disparate departmental agencies

   In carrying out its mission, the Department administers and enforces more than 180 Federal laws. These mandates and the regulations that implement them cover workplace activities for about 8.5 million employers and 143 million workers. With a budget of 51 billion dollars and over 21,000 employees and contractors nation-wide, we are an organization of distinct agencies that in many cases operated autonomously, and with varying supporting IT systems.

3. Cultural behaviors not conducive to a common security posture

Our next challenge was to change the behavior of managers, including due attention to IT security as a key part of everyday business. We worked to make managers more aware of security concerns. To that end the following actions were carried out:

- In 2001, a Security Manager was hired and placed in the OCIO to manage the Department-wide security program. That manager set high standards for our Department Computer Security Program and worked with agency counterparts to develop consistent and achievable security processes and procedures.
- In 2002, the DOL IT Security policies and procedures were updated to incorporate current OMB and NIST guidelines.
- In 2003, the Department established a permanent Technical Review Board IT Security Subcommittee, comprised of agency security managers and technical support to address Department-wide security issues.
- In 2003, Secretary Elaine Chao issued Secretary's Order 3-2003, *Update of Delegation of Authority and Assignment of Responsibility of the Chief Information Officer*, dated May 16, 2003, outlining the roles and responsibilities for management of information technology at DOL to include IT security responsibilities.
- In 2003, the Department developed an eGovernment Strategic Plan that ties IT Security to the Department's mission. This plan was published on the Department's website.
- In 2005, the Department updated the DOL IT Strategic Plan where IT Security goals and direction are incorporated. This plan was published on the Department's website.

Computer Security Program Status and Successes

At the Department of Labor, the Assistant Secretary for Administration and Management (ASAM) also serves as the Chief Information Officer (CIO). The combination of the CIO responsibilities and the ASAM responsibilities affords distinct advantages in the implementation of the Clinger-Cohen Act. As a result, we are in a good position to link proposed IT investments to Departmental missions, priorities, and strategies and ensure the integration of IT policies and plans cohesively throughout the Department.

At DOL, our Computer Security Program has progressed from a grade of "F" in 2001 to a "B-" in 2004. This improvement is due to the strong support of the Secretary of Labor, DOL senior management, and our Departmental Information Technology (IT) professionals. Additionally, our Computer Security program was a significant contributor to the Department's achieving and maintaining a "Green" rating on Expanded Electronic Government on the President's Management Agenda scorecard.

The successes we have achieved to date can be attributed to strong oversight of Department-wide security issues, cooperation at the IT senior management level, and

continuous collaboration through Department-wide review boards. The DOL Technical Review Board (TRB), comprised of permanently assigned agency representatives, serves as the Department's first tier Investment Review Board for major IT investments and as a forum to identify and resolve Department-wide IT-related issues, including computer security. Recognizing the overarching importance of IT security, in early 2003 a new permanent DOL IT Security Subcommittee was formed to address Department-wide IT security issues. The efforts of the DOL IT Security Subcommittee resulted in sound security practices that enable consistent FISMA reporting from the OCIO and the Office of the Inspector General (OIG), to which we attribute the following successes:

- A fully integrated Computer Security program -- Capital Planning and Investment Control (CPIC), Enterprise Architecture (EA).
- Revised DOL System Development Lifecycle Management Manual to incorporate IT security requirements at each phase of a systems lifecycle. (December 2002)
- Received OIG approval for the Department's Plan of Action and Milestones (POA&M) program (since 2003).
- Revised DOL EA to incorporate security at each layer (May 2005)
- CPIC Control reviews – ensures adequate IT security expenditures.
- Semi-annual eGovernment reviews of all DOL agencies modeled on the PMA scorecard and FISMA performance metrics – ensure effective agency security program performance.

The cornerstone of the Department's Computer Security Program is the National Institutes for Science and Technology (NIST) Special Publication (SP) 800-26 -- *Security Self-Assessment Guide for IT Systems* and NIST 800-53 -- *Recommended Security Controls for Federal Information Systems*. Correspondingly, the Department has maintained a comprehensive Certification and Accreditation (C&A) program, achieving:

- Authority to Operate (ATO) -- not just interim authority--for 100% of our major information systems – up from 97% in FY2004.
- Contingency Plan testing for 100% of our IT system Contingency Plans – up from 73% in FY2004.
- Security Controls Testing and Evaluation for 100% of our IT systems – up from 91% in FY2004.
- The completion of specialized, role-based IT Security training for 94% of our employees with significant security responsibilities – up from 57% in FY 2004.

Areas of Improvement

Despite this progress in securing our IT systems at DOL, we recognize that security is a constant challenge and a task that can never be considered complete. In addition to day-to-day measures to protect our IT assets, we have identified three areas for strengthening our Computer Security Program:

- general and application security controls
- patch management
- IT security manager competencies

The Department has developed a comprehensive work plan to address these issues to include:

- The implementation of NIST 800-53
- The Certified Information Systems Security Professional training and certification exam for DOL security managers

We are confident that we will achieve meaningful improvements this fiscal year.

In conclusion, computer security is a core element of our business and culture at the Department of Labor. Secretary Chao, Deputy Secretary Law, Chief Information Officer Pizzella, agency senior management, and the dedicated DOL IT professionals are committed to the Department's Computer Security Program, and will continue to ensure resources are adequately applied for the proper protection of our information systems. As we are faced with the evolution of FISMA compliance, we will strive to maintain a balance of FISMA reporting requirements and the implementation of sound security practices.

Mr. Chairman, thank you for the opportunity to provide a brief outline of DOL's approach to Information Security. I would be happy to answer any questions.

Chairman TOM DAVIS. Thank you very much.
Mr. Lentz.

STATEMENT OF ROBERT LENTZ

Mr. LENTZ. Good afternoon, Mr. Chairman and members of the committee. As Chief Information Assurance Officer for the Department of Defense, I appreciate this opportunity to highlight the posture of information security within the Department.

The Department leadership is fully engaged in the security efforts in support of FISMA. Secretary Rumsfeld considers information technology a critical strategic component in transforming America's armed forces for the 21st century warfare. Our recently completed Quadrennial Defense Review stresses networks and information security as key areas of focus.

Collaboration between the CIO and the war-fighting community is absolutely critical. The protection of the network is everybody's business. This can't be overstated. We take specific actions to train, license, qualify, and certify pilots and weapons systems. We must consider no less a standard for the operation, security, integrity of our information systems.

The DOD IA strategic plan has for 3 years been institutional component driving strategic objectives for improving our security posture. It also enables FISMA compliance. The Department of Defense uses FISMA as a critical management and assessment tool. We continue to enhance our FISMA efforts.

The Department reviewed over 3,500 systems this past year, an increase of more than 1,000 systems from 2004. The Department increased its Authority to Operate rate from 58 percent in 2004 to 82 percent in 2005. In addition, our Total Accreditation rate was at 93 percent.

Last year, more than 2 million of the approximate 2.6 million DOD personnel who had access to DOD networks received IA security awareness training. This training was accomplished even while larger members of the servicemembers were deployed to combat theaters. In addition, more than 67,000 individuals with significant security responsibilities received specialized security training.

I have identified in the full written testimony many initiatives that DOD has undertaken to improve its Information Security Department. Let me highlight a few others.

The Department is aggressively pursuing an enterprise architecture and prioritized enterprise solutions through centralized funding.

The Department has comprehensive policies and process for system configurations, a very important area. One example is the distribution by the Air Force of Microsoft software with standard security configuration resulting in improved network security and management.

Departmental components are accelerating the use of public key infrastructure, from network access and secure log-on, consistent with HSPD–12. Over 3 million personnel are outfitted with common access cards, enabling PKI capabilities throughout the Department.

In 2005, the DOD published a comprehensive IA Workforce Improvement program, launching an aggressive effort to certify nearly 80,000 core network professionals.

As to identified security weaknesses in this year's FISMA report, we are pleased to advise you of the following remedies: Considering the dynamic operational environment of DOD and the sheer number of systems deployed across the enterprise, we have made significant progress in the area of inventory of our IT systems. We believe that our inventory of major information systems is under control.

Regarding the challenges of instituting a process for managing plans of actions and milestones, the Department has a PO&M process that was improved in 2005 from lessons learned and from IG audits. We continue to improve that process by making this year's guidance more detailed and integrated into our C&A guidance as well.

We are also developing an automated standardized capability that will add greater visibility to PO&Ms.

We believe the Department certification and accreditation process is very solid and getting better. FISMA delegates authority to the Secretary of Defense to develop security policy and guidelines for all of its information systems. The DOD C&A process is consistent with NIST guidelines but designed to address classified national security systems and factor in unique operational challenges.

In the area of training in 2005, the DOD components reported a total of 79,000 employees with significant IT security responsibilities. In such a large, dynamic, and changing organization that number will always be in a state of flux.

In conclusion, the Department of Defense is committed to a strong and comprehensive security program. Our commitment to improve our FISMA compliance is an essential element of the Department's information security strategy.

Again, I thank you for the opportunity to comment on this important topic.

[The prepared statement of Mr. Lentz follows:]

Statement by

Robert F. Lentz

Director, Information Assurance

Assistant Secretary of Defense for

Networks and Information Integration

Before the

House Government Reform Committee

Hearing on

Information Security and

Implementation of the Federal Information Security Management Act of 2002

March 16, 2006

For Official Use Only

Until Release by the

Committee on Government Reform

U.S. House of Representatives

Thank you, Mr. Chairman and distinguished members of the Committee for this opportunity to testify before your Committee on Government Reform on the subject of Information Security and the Department of Defense's implementation of the Federal Information Security Management Act (FISMA) of 2002. I am Robert Lentz and this is my first opportunity to appear before you as the DoD Senior Information Assurance Officer. My prepared remarks cover the status of DoD's information security program and implementation of FISMA in the challenging cyber threat environment of the 21st Century.

To respond to this increased pace of cyber threats, technological change and evolving operational demands, the Department has integrated multiple programs and initiatives into an overarching approach protecting DoD information. DoD is leveraging the congressional reporting requirements under FISMA as a principal management and assessment tool to monitor and improve its IT security posture.

The Secretary of Defense's guidance has been that the protection of information and networks is fundamental to ensuring the success of warfare today. He has also emphasized that our adversaries have not been idle. Most of them know that they cannot defeat the United States military on a conventional battlefield, so they see cyber attacks as an inexpensive means of leveling that battlefield. These asymmetrical threats are real and the results of insecurity are potentially catastrophic.

To enable the transformation needed to meet the challenges posed by today's new threat environment, the Department's vision is of a single, secure grid providing seamless end-to-end information exchange capabilities to all warfighers, policy-makers, and support personnel that we call the Global Information Grid (GIG). The Department is leveraging emerging information technology to create this seamless, interoperable, network-centric environment. To translate that information technology into combat power, the Department is translating information technology into combat power and is migrating from platform-dependent to network-centric operations.

We must protect our information from threats: enemy, criminal, insider, or self-inflicted accidental events that weaken our security. Our information base and our ability to leverage the technology to support warfighting, intelligence, and business functions must have the highest level of trust and confidence or we lose the advantage that information provides us.

The GIG is a network of unprecedented complexity. It crosses organizational boundaries internal and external to the Department of Defense. The GIG is composed of an extensive variety of computers, communications hardware, and vast numbers of ancillary equipment. The responsibility for managing and operating these technologies and hardware extends across many DoD organizations and into many of our commercial partners.

The protection of the GIG is everyone's business - this cannot be overstated. We take specific actions to train, license, qualify, and certify pilots and weapons systems operators to a very high standard - we must consider no less of a standard for those who

operate, and ensure the security and integrity of the GIG. "Fighting the Net" is the commanders' business, but "Protecting the Net" is everyone's business.

Meeting Challenges

Our objective is to support defense and national security requirements through all levels of conflict and contingency support. Network-centric operations bring together joint, high-capacity networked operations and weapons systems, merging key tactical and strategic functional capabilities. The GIG supports all DoD missions, including joint and combined task-force commands, with the most effective, assured, and secure information-handling capabilities possible.

The Department's vision is to foster an agile, robust, interoperable and collaborative environment, where warfighters, business, and intelligence users all share knowledge in a secure, dependable and global net-centric environment that enables informed decision-making and effective operations. We will empower individuals at the edge of the network by providing them immediate access to information, and incorporating the information they provide into the GIG, while exploiting the weaknesses of enemies who are denied a comparable advantage. As part of DoD's information age transformation, the network is emerging as the most important contributor to combat power and force protection.

The DoD IA Strategic Plan

Because DoD is so large and complex, a comprehensive IA Strategic Plan is necessary to present an integrated view and consistent approach to security across the enterprise. The DoD IA Strategic Plan serves as the IA planning and management guide

for all Combatant Commands, Services, and Defense agencies. It establishes the Department's IA goals, sets out strategic objectives for IA, and provides a consistent approach to assuring information across the DoD enterprise and complying with FISMA. The IA Strategic Plan has five goals:

- Protect information to safeguard data (as information) as it is being created, used, modified, stored, moved, and destroyed, at the client, within the enclave, at the enclave boundary, and within the computing environment, to ensure that all information has a level of trust commensurate with mission needs.
- Defend systems and networks by recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies, ensuring that no access is uncontrolled and that all systems and networks are capable of self-defense.
- Provide integrated IA situational awareness/IA Command and Control (C2), integrating the IA posture into a user-defined operational picture (UDOP) synchronized with network operations (NETOPS) and emerging Joint C2 programs to provide decision makers and network operators at all command levels the tools for conducting Information Assurance/Computer Network Defense operations in net-centric warfare.
- Transform and enable IA capabilities innovatively by discovering emerging technologies, experimentation, and refining the development, delivery, and deployment processes to improve cycle time, reduce risk exposure, and increase return on investments.

- Create an IA-empowered workforce that is well equipped to support the changing demands of the IA/IT enterprise.

The DoD IA Policy Framework

The Department has developed an IA policy framework that provides overarching IA policy and procedural guidance to implement the IA Strategic Plan. The capstone Department of Defense Directive (DoDD) 8500.1, *Information Assurance*, was issued in October 2002. DoD Instruction (DoDI) 8500.2, *Information Assurance Implementation*, was issued in February 2003. Since then, additional policies that provide more detailed guidance on specific functional areas have been issued. They include such topics as computer network defense, certification and accreditation of all DoD systems, training and certification of the IA workforce, the DoD public key infrastructure, integrating IA into defense acquisition, IA for space systems, and biometrics.

Areas of Significant Improvement

The DoD has taken significant steps to address new threats and shortcomings in the defense of the GIG. Initiatives include:

Enterprise Solutions - The Department is aggressively pursuing prioritized enterprise solutions through centralized funding across all agencies, accelerating the implementation and closure of capability gaps. The Department has an effective defensive posture against cyber attacks. The Department selects and implements enterprise-wide computer network defense tools that automatically identify and remediate vulnerabilities, detect anomalies, mitigate insider threats,

and eliminates spyware. A number of additional products are being provisioned for enterprise deployment.

Configuration Management - The Department has comprehensive policies and processes for system configuration. One example is the distribution by the Air Force of Microsoft software with standard security configurations service-wide, resulting in improved network security and management The Department is aggressively moving toward a standard configuration management process similar to the successful efforts of the Air Force. As this concept proves itself over time, the Department will assess and may adopt similar processes for the enterprise.

The DoD has robust policies and processes for system configuration. The Defense Information System Agency (DISA) Field Security Operations develops Security Technical Implementation Guides (STIGs) for critical IT products. The DISA STIGs provide security configuration guidance for Windows NT, 2000, and 2003; UNIX (includes Solaris, HP-UX, and Linux); Database (includes Oracle and SQL Server); Network Infrastructure (includes Cisco IOS and Juniper IOS); and many other technologies such as OS/390, Web Servers (IIS, Netscape), Voice over Internet Protocol, Biometrics, Domain Name Server (DNS), Unisys, and Tandem.

Another aid to the standard configuration of machines by DoD is a DISA-developed product known as the "Gold Disk," which is based on the STIGs. This government-developed product is intended to help System Administrators determine the configuration of a computer and then help them automatically fix most configuration vulnerabilities. Because configuring a system to the DoD

standard can be labor-intensive and prone to error, the potential benefits to the Department are significant.

Public Key Infrastructure (PKI) - Departmental components are accelerating use of Public Key Infrastructure for network access and secure login. Over 3 million personnel are outfitted with Common Access Cards enabling PKI capabilities throughout the Department of Defense population.

We are now implementing PKI-based logon, which will increase the difficulty for adversaries to remotely access Department systems. Upcoming requirements include integrating DoD PKI security services at multiple levels to include DoD websites to lessen the likelihood of unauthorized disclosure of DoD information.

Password Stand-Down – The CIO has emphasized the need to implement CAC/PKI single sign-on to networks. On November 29, 2005 the Joint Task Force-Global Network Operations (JTF-GNO) directed a DoD-wide Network Stand-Down Day to require DoD elements to confirm all accounts and users were required to change passwords or their accounts were locked.

DoD IA Workforce Management - The Department recently published the DoD IA Workforce Improvement Program Manual, DoD 8570.01M, establishing a Department-wide IA standard for IA workforce management and baseline knowledge and skills that all personnel performing IA functions including military, civilians and contractors must meet . This manual leverages industry best practices and raises the bar on IA certifications by requiring they be accredited by

the American National Standards Institute (ANSI) to meet the International Organization for Standardization/International Electro-technical Commission (ISO/IEC) standard 17024, *General Requirements for Bodies Operating Certification of Persons.*

- The DoD IA Scholarship Program (IASP) was established in 2002 to attract and retain top talent and to target academic research to support the mission critical IA/IT needs of the Department. Since its inception, 206 students have been in the DoD IA Scholarship Program (IASP). Through March 2005, 65 have graduated and either are working in DoD or have completed their obligation.
- Instituted the Centers of Academic Excellence in Information Assurance Education program; and expanding it from 23 universities in 21 States in 2002, to 66 universities in 27 States today. These include 4 DoD schools (US Military Academy, US Air Force Academy, Air Force Institute of Technology, and Naval Postgraduate School)

Vulnerability Management Process - DoD is employing an aggressive approach to patch management and vulnerability mitigation across the enterprise. DoD has implemented a process called the Information Assurance Vulnerability Alert (IAVA) Management Program to mandate the rapid application of software patches and configuration changes when security vulnerabilities are identified. The IAVA process requires the Combatant Commands, Services, and Defense agencies to update configurations to incorporate the new patches or to take other

vulnerability remediation actions directed by the JTF-GNO. In turn, Components report their compliance with these security mandates.

While patching and configuring tens of thousands of devices (servers, routers, computers, etc.) can be challenging, DoD has taken significant steps to make configuration change easier and more certain. DISA has established a distribution system for the dissemination of security-relevant patches throughout the enterprise. Patch repositories and antivirus distribution servers are available on the classified and unclassified GIG networks. These repositories enhance DoD's ability to protect against newly announced vulnerabilities because DoD is no longer competing with the entire Internet community for access to vendor-released patches. DoD users have exclusive access to the repositories, thus speeding up the overall response.

Ports, Protocols, and Services - The Department made significant strides in managing network Ports and Protocols. In concert with JTF, the Department established an enterprise program to eliminate unofficial traffic entering and leaving the GIG. These efforts close unused ports, stop the use of vulnerable computer communication protocols that could easily allow hackers to access our systems, and reduces the risk of potentially malicious traffic entering and leaving the Global Information Grid (GIG).

Host (workstations and servers) Vulnerability Scanning and Remediation - In 2005 the DoD purchased and deployed two enterprise software tools that permit system administrators to scan and report compliance with DoD vulnerability patch

policies and push patches to remote machines. These two tools reduce time to patch security holes being exploited by our adversaries and for senior leaders to verify compliance across the Department.

Host Based Security System (HBSS) - HBSS is a host based intrusion prevention system to increase the difficulty for adversaries to compromise DoD hosts. Additionally HBSS permits system administrators to repeatedly baseline their systems and compare baselines to discover changes that indicate adversary activity. HBSS is currently going through source selection and contracting.

Spyware - In July 2005, DISA awarded a contract for a DoD enterprise-wide anti-spyware solution to complement its very successful enterprise anti-viral capability. The solution will be used by System Administrators and cyber-security personnel throughout the Department, including the DoD-related intelligence agencies, the National Guard, and the Reserves.

Enhanced Inspection Program - The Department is increasing the scanning of DoD networks to discover networks in violation of DoD policies; the Department will direct actions to mitigate deficiencies.

Enterprise Intrusion Detection Systems - The Enterprise Solutions Steering Group (ESSG) in coordination with DISA and JTF-GNO is allocating new sensors for DoD components to improve the current DoD enterprise sensor grid and established tighter sensor configurations on backbone networks.

Network Mapping - The JTF-GNO is enabled operations of a DISA automated network mapping capability to improve situational awareness of the DoD enterprise networks.

Incident Handling - The Joint Staff updated incident handling guidance formalizing the current ad hoc processes across the communications, operations, law enforcement, counter-intelligence, and intelligence community. Additionally this policy requires operational commanders and leaders to report incidents impacting mission effectiveness or support of deployed and contingency force operations through operational channels in addition to communications channels.

Information Condition (INFOCON) Policy - The DoD INFOCON policy is an alert and response system designed to permit the Commander, US STRATCOM to assess and respond to enterprise-wide cyber threats.

Status of Information Security and FISMA Implementation in DoD

The Department of Defense uses FISMA as a management and assessment tool to improve its IT security posture. The Defense-wide Information Assurance Office (DIAP) is responsible for oversight of the Information Assurance program for DoD. In addition, the DIAP orchestrates the FISMA process with representatives from all the DoD reporting Components, which include the Military Services, the Combatant Commands, DoD Agencies, and DoD Field Activities.

The Department continues to enhance its FISMA effort consistent with guidance from OMB. Specifically:

- The Department continues to add mission support systems to its reportable inventory and reviewed over 3,500 systems in Fiscal Year 2005 – an increase of more than 1,000 systems from Fiscal Year 2004.
- The Department increased its Authority to Operate (ATO) rate from 58% in Fiscal Year 2004 to 82% in fiscal year 2005. In addition, our total Accreditation rate (ATO/IATO) was 93 percent.
- The Department is including a detailed POA&M process in the FY06 DoD FISMA guidance. These improvements let us better track and analyze systemic issues.
- Last year, more than 2 million of the approximately 2.6 million DoD military, civilian, and contractor personnel who had access to DoD networks received documented IA security awareness training. This training was accomplished even while larger numbers of Service members were deployed to combat theaters. In addition, more than 67,000 individuals with significant security responsibilities received documented specialized security training.
- The DoD IT Portfolio Repository (DITPR) is the database of record for the FISMA system reporting. The OSD uses the DoD IT Portfolio Repository (DITPR) to compile the system metrics of the FISMA report. In accordance with Deputy Chief Information Officer Memorandum December 21, 2004, all Mission Support systems are being entered into the data base by the end of Fiscal year 2006.

Identified Security Weaknesses and Remediation

In the current year FISMA report, the DoD Office of the Inspector General (OIG) identified the following areas as deficient. I will address these areas specifically, and offer our status or remediation effort.

Issue: The OIG has stated that DoD lacks an inventory of major information systems, with identified interfaces, including those not under control of the agency.

Response: We believe the inventory of major information systems under the control of the Department is as accurate as possible considering the dynamic environment and sheer number of systems deployed across the DoD enterprise. We are also continuing the effort to complete a comprehensive enterprise-wide inventory, including mission support systems.

Issue: The IG has stated that the Departmental Plan of Actions and Milestones process is not an agency wide process, incorporating all known IT Security weaknesses.

Response: The Department has developed comprehensive POA&M guidance that has been integrated into the Fiscal Year 2006 DoD FISMA guidance and will be incorporated into a permanent DoD policy issuance in the near future.

Issue: The IG has stated that the quality of DoD Certification and Accreditation (C&A) process is poor and believes that DoD should be following NIST, rather than DoD policy and guidance.

Response: This issue is in the process of being addressed. Section 3543 (c) of FISMA delegates authority to the Secretary of Defense to develop security policies and guidelines for all DoD information systems. The DoD C&A process is currently under

revision. It is consistent with NIST guidelines but it is more extensive and has a somewhat different orientation because it must address classified national security systems as well as the non-national security systems covered by NIST guidelines.

Issue: The IG has stated that the Department is not aware of the number of employees with significant IT Security responsibilities.

Response: The DoD Components reported a total of 79,986 employees with significant IT security responsibilities in FY05. In such a large and dynamic organization, that number will always be in flux. However, in our continued drive for effective workforce management, the Department has established a comprehensive process under the newly issued DoD training and workforce improvement manual to account for and track all IT security personnel and IT security certifications in order to reflect the most accurate number possible.

What are the greatest obstacles to addressing these weaknesses?

Considering the size, complexity, and dynamically changing operational tempo of the Department of Defense, the Office of the CIO considers the greatest obstacles to be keeping up with the asymmetric threat landscape, and our ability to defend the network in an agile manner.

What Additional Guidance, Procedures, or Resources the Department Feels It Needs to Improve Its Information Security and FISMA Compliance?

For large organizations such as the Department of Defense, the FISMA IG review should take the form of an assessment rather than a formal audit. Additional guidance toward this goal can be offered to assist in standardizing IG FISMA assessments across

all federal agencies. Additionally, the dynamic environment of The Department of Defense requires unique policies and procedures.

Conclusion

The Department of Defense is committed to a strong and comprehensive security program. The Department continues to move forward to address enterprise solutions necessary for protecting its information systems and networks. Our commitment to improve our FISMA compliance is an essential element of the Department's information security strategy.

Again, I thank you for the opportunity to comment on this important topic and I look forward to answering any questions you may have.

Chairman TOM DAVIS. Thank you very much.
Mr. Charbo.

STATEMENT OF SCOTT CHARBO

Mr. CHARBO. Thank you, Mr. Chairman and committee members. My remarks will cover the current status of the Department's implementation of FISMA.

The mission of the Department of Homeland Security's information security program is to provide the Department with a secure and trusted computing environment that enables the Department to leverage information technology and effectively and securely share information in support of its many and varied missions. Statutory compliance is a top priority, and the Department's information security program is structured around compliance with FISMA as well as OMB in this guidance.

In 2003 and 2004, the Department laid the necessary foundation of effective security policies and architecture guidance. Policies are now codified in a dedicated management directive and a systems security architecture is fully integrated with the Department's architecture.

Security policies and architectures are both updated on a regular basis and compliance is enforced through the use of several mandatory security management tools that are now in use throughout the Department. Building on those efforts, the Department completed three major information security initiatives in 2005.

First, a comprehensive systems and applications inventory was completed in August 2005. The inventory is based on a detailed methodology for identifying systems and applications using standard Federal definitions. This inventory now provides clear accreditation boundaries for each and every operational IT system and assigns responsibilities for those controls to specific individuals, thereby providing a baseline for measuring security compliance.

To ensure the inventory remains accurate, annual inventory reviews will continue each year, with a near-term focus on 2006 of linking the inventory to the Department's capital planning and investment control processes, thus allowing the Department to better integrate effective security controls at the beginning of a system's life cycle.

In the Department's fiscal year 2005 FISMA report, the Inspector General acknowledged for the first time the completeness and accuracy of our FISMA inventory.

Second, an enterprise certification and accreditation tool was successfully fielded in April 2005, and that is now fully integrated with a FISMA management tool fielded in 2004.

Third, a comprehensive and repeatable set of information security metrics significantly improved system owner accountability. These metrics now measure and inform progress in completing the accreditation of all operational systems. Monthly information security scorecards provide detailed status updates to Department leadership, and these scorecards are highly successful in improving the accountability of system owners.

These three initiatives build on earlier milestones and have now paved the way for real, measurable cyber security improvements. The Department implemented an aggressive remediation project

for 2006 with a goal of 100 percent remediation by the end of this year. Originally announced by Secretary Chertoff in his keynote address at the Department's annual Security Conference last August, the project moved into full swing in October 2005 and the Department is on its way to full remediation.

The Department's FISMA inventory currently includes approximately 700 systems, and prior to the initiation of the remediation project, the number of fully accredited systems was only 26 percent. By the end of February of this year, over 60 percent of those systems are now fully accredited. In just 5 months, the Department has more than doubled the number of accredited systems and it is on track to make the goal of full remediation by the end of the year. It is clear the project is positively affecting the security culture of the Department, and recent upward trends in remediation metrics support the view.

The Department must also ensure those systems and applications are connected across a secure enterprise backbone providing shared IT services. To accomplish this goal, an aggressive infrastructure transformation program called One Net was initiated for 2006 to bring all legacy information technology infrastructures under a single enterprise. Benefits of One Net include network optimization and improved quality of service, both of which will significantly enhance information sharing initiatives.

Planning for One Net began with a comprehensive security framework that is consistent with the detailed systems security architecture of the Department.

As part of the One Net effort, the Department is also fielding its first enterprise-wide network operations and security center. The center is responsible for managing the Department's shared IT enterprise environment in real time, including the discovery and remediation of security incidents as they occur, and represents a significant improvement to our overall security posture.

I am confident that the DHS information security program is moving in the right direction.

Thank you. I look forward to your questions.

[The prepared statement of Mr. Charbo follows:]

Statement by

Scott Charbo

Chief Information Officer

Department of Homeland Security

Before the

House Government Reform Committee

Hearing on

Information Security and

Implementation of the Federal Information Security Management Act of 2002

March 16, 2006

Thank you Mr. Chairman and Members of the Subcommittee for allowing me this opportunity to testify before the House Committee on Government Reform on the subject of Information Security and the Department of Homeland Security's implementation of the Federal Information Security Management Act (FISMA) of 2002. My prepared remarks will cover the status of the Department's implementation of FISMA.

The mission of the Department of Homeland Security's Information Security Program is to provide the Department with a secure and trusted computing environment that enables the Department to leverage Information Technology (IT) and effectively and securely share information in support of its many and varied missions. To this end, statutory compliance is a top priority, and the Department's Information Security Program is structured around compliance with the Federal Information Security Management Act (FISMA), as well as Office of Management and Budget, and National Institute of Standards and Technology guidance.

The Department's Program has come a long way in just three short years. In 2003 and 2004, the Department laid a necessary foundation of effective security policies and architecture guidance. Policies are now codified in a dedicated Management Directive and the systems security architecture is fully integrated into the Department's Enterprise Architecture. Security policies and systems security architecture are both updated on a regular basis, and compliance is enforced through the use of several mandatory security management tools that are now in use throughout the Department. These early program-development steps have given the Department an important foundation, and building on those early efforts, the Department completed three major information security initiatives in 2005.

First, a comprehensive systems and applications inventory was completed in August 2005. The Department-wide FISMA inventory is based on a detailed methodology for

identifying systems and applications using standard federal definitions. This inventory now provides clear accreditation boundaries for each and every operational IT system supporting the Department's diverse missions and assigns responsibility for security controls to specific individuals, thereby providing a baseline for measuring security compliance. To ensure the inventory remains accurate, annual inventory reviews will continue each year with a near term focus in 2006 of linking the inventory to the Department's capital planning and investment control processes, allowing the Department to better integrate effective security controls at the beginning of the systems' life-cycle. In the Department's fiscal year 2005 FISMA report, the Inspector General acknowledged for the first time the completeness and accuracy of our FISMA inventory.

Second, an enterprise certification and accreditation tool was successfully fielded in April 2005, and that is now fully integrated with a FISMA management tool fielded in 2004. These tools automate many of the day-to-day security tasks associated with FISMA compliance, thereby easing the security burden on system owners. The result is a consistent and cost-effective set of security management procedures in use throughout the Department.

Third, a comprehensive and repeatable set of information security metrics significantly improved system owner accountability. These metrics now measure and inform progress in completing the accreditation of all operational systems, as well as other key compliance activities throughout the Department. Monthly information security scorecards provide detailed status updates to Department leadership, and these scorecards are proving highly successful for improving the accountability of system owners.

These three initiatives build on earlier milestones and have now paved the way for real and measurable cyber security improvements in the near future. With momentum from these initial successes, the Department implemented an aggressive Remediation Project for 2006, with a goal of 100% remediation by the end of the year. Originally announced by Secretary Chertoff in his keynote address at the Department's annual Security

Conference last August, the Project moved into full swing in October 2005, and the Department is well on its way to full remediation.

The Department's FISMA inventory currently includes approximately 700 systems, and prior to the initiation of the Remediation Project, the number of fully accredited systems was only 26% Department-wide. By the end of February of this year, over 60% of the systems are fully accredited. In just 5 short months the Department has more than doubled the number of accredited systems, and it is on track to make the goal of full remediation by the end of this year. It is clear the Project is positively affecting the security culture of the Department, and recent upward trends in remediation metrics support that view.

Until now, I have only addressed Program-specific, systems-and-applications security compliance initiatives. However, the Department must also ensure those systems and applications are connected across a secure enterprise backbone providing common shared IT services. To accomplish this goal an aggressive Infrastructure Transformation Program called "OneNet" was initiated for 2006, to bring all legacy information technology infrastructures under a single enterprise program. Benefits of this approach are many, to include network optimization and improved quality-of-service, both of which will significantly enhance information sharing initiatives. The enterprise will operate at considerably lower life-cycle costs in the future.

Planning for "OneNet" began with a comprehensive security framework that is consistent with the detailed systems security architecture of the Department. The Department's security framework provides systems owners with common, shared enterprise IT services, where information at differing sensitivities and users at differing levels of trust have assured information sharing through the use of Security Trust Domains. This framework now provides a strong security foundation from which to build upon in the future, and enhanced security represents the single biggest benefit from the OneNet Project.

As part of the "OneNet" effort, the Department is also fielding its first enterprise-wide network operations and security center. The center is responsible for managing the Department's shared IT enterprise environment in real-time, including the discovery and remediation of security incidents as they occur, and represents a significant improvement to our overall security posture.

I am confident that the DHS Information Security Program is moving in the right direction and I look forward to working with you and your staff in the future, as, together, we "secure the success of DHS."

Thank you and I look forward to your questions.

Chairman TOM DAVIS. Thank you, all.

Now, looking at the report card, we seem to have a reverse bell curve, with agencies settling at either the high end or the low end. For the two over here on my left, or on the right here, what are the major steps your agency took to achieve it? You didn't start off with A's, you worked steadily toward that. And I would say for DOD and then DHS, what are the major challenges you feel prevent you from progressing? Your plan for addressing these challenges you alluded to in your comments, what would you like to see your partners in this process do to help you? I am talking about OMB, GAO, and the IG.

I will start with you, Mr. Hughes. You traced out the things you did to get your A+ and maintain it.

Mr. HUGHES. Mr. Chairman, members of the committee, really, at Social Security there is a strong emphasis on security. It has been there for many years, as I have repeated. And with FISMA, I can tell you we take it very seriously. We meet regularly, we constructively argue regularly, and we try to make corrections. So you have to make that commitment to keep challenging, as executives, the importance of security and that FISMA is a real exercise. And so I don't know if I can say that enough from a practical reality. It is not a paper report, it is real security that we are trying to constantly be aware of. And that is what FISMA teaches us.

Chairman TOM DAVIS. Mr. Wiesner.

Mr. WIESNER. At the Department of Labor I would have to say there are a few items that have led to our success. One is the strong leadership and management commitment from the Secretary's level through all the levels of management, including assistant secretaries, the various senior IT management staff within the Department of Labor. And it starts at the top and management supports us 100 percent in ensuring that we protect our departmental assets.

The second step we have done over the last few years is really integrate IT security into our IT management processes, procedures, and governance models. We start looking at security at the capital planning stage and enterprise architecture, during the systems development life cycle process, the entire life cycle. So we put security integrating into every IT project that we undertake and currently the ones that are under way.

And then the other thing we have worked on really hard is to establish a strong relationship with the OIG, recognizing that they have a strong compliance role and they have their views on how they view us as being successful and the things that they discover in their audits and what we should be focusing on, and we establish that relationship and try to form a partnership so we are heading in the right direction.

Chairman TOM DAVIS. Thank you.

Mr. Lentz, let me just ask you, I mean, if you had an A+ you would feel your agency was more secure, wouldn't you?

Mr. LENTZ. Of course, sir. I think the question you asked in your earlier panel, sir, I think goes to the heart of one of the challenges that we have, which, as you said earlier, a very large and a very diverse, dynamic organization that is deployed worldwide and things are changing all the time.

I think the discussions that I have had with my peers, other chief security officers in the Department as well as private-sector leaders in this area, I think the point that has to be emphasized is that during the FISMA process, the act calls for an assessment, not an audit. An assessment takes into account a lot of factors. In a large organization like the Department of Defense—or Homeland Security, for that matter—you have a changing environment. Where an audit could in fact pick up one or two systems that may not be accounted for or a certain number of personnel that may be deployed that are achieving certain status, you know, I think through that kind of dynamic environment, it makes it very difficult to, at some times, achieve the kind of scores that may be indicative through an auditive process.

I think by working closely with the IG, which is indicated by my colleagues, I think that is a very important step in this process and one that we are continuing to strive for.

Chairman TOM DAVIS. One of the things is, when we got our reports on DOD, we got like four different reports. We get the Army, Navy, Air Force. I mean, it kind of made up just the way that your organization is different from a lot of other agencies in terms of how this is compiled and so on. I mean, is that an obstacle?

Mr. LENTZ. I think Secretary Rumsfeld through the QDR process and our new CIO, Mr. Grimes, wants to remove any type of obstacle that may in fact be inferred by that kind of service-oriented environment that we live in. We are very much focused on an enterprise architecture, we are very much focused on an enterprise CIO governance model. And I think we are already seeing improvements in that area already that I think are going to be reflected very much so in next year's report, sir.

Chairman TOM DAVIS. OK.

Mr. Charbo, I will ask you, I mean, obviously you come from a—you had a number of dysfunctional agencies you are trying to put together. You have had a steep climb over there to begin with. So I concede that to you.

Mr. CHARBO. Thank you. I think the first thing that we have done—and our numbers, I think, are supporting that we are moving in the right direction right now, in the last 5 months. We have been able to move it more than it has moved in the last couple of years.

But the first piece that we had our teams accept was where we were was not where we wanted to remain. So we admitted that we weren't in the right posture that we wanted to have moving forward in terms of the security of our systems. So we asked Secretary Chertoff to lead that charge for us at our annual conference and then place that accountability to those system owners in the multiple components that we have.

We have seen very good response from the Coast Guard and Customs, ICE. Even FEMA has responded well in terms of the accountability for securing the systems.

Publishing the inventory was a major milestone for us. It put that benchmark in the sand. Now we are focused on moving that forward. And I guess I would just say, we use a term called "relentless" in the Department. You will get a lot of excuses on how hard

this is to do, but we accept that but we still need to move it forward. And that is what we are focused on.

Chairman TOM DAVIS. But GAO reported that there was a very low level of security incident reporting in DHS. What is the problem? What is the deterrent here? Do we need to do anything to remove those barriers?

Mr. CHARBO. I think we have rallied that in here in the last 5 months. We have implemented policies, we have done some training with our systems security professionals that we have in the Department, and we have worked through those processes to assure that we are getting reporting.

The other piece that I think will really improve that is how we are going to be monitoring our systems. We have had multiple wide-area networks. So you have different methodologies of reporting. That is now coming through a core NOC-SOC—network operations, security operations center—through our One Net. And they will have a responsibility of moving that to the US-CERT.

Chairman TOM DAVIS. One of the problems you have at DHS is you have taken all these disparate agencies, over 100 and some 1,000 employees, and put them together, and everybody expects immediate results. This is a work in progress. I mean, this takes years, doesn't it, as a practical matter?

Mr. CHARBO. We are going to take 1 year to certify the systems. We will move those, a large milestone—as we say in our statement, we were at 26 percent that we could document and we are now about 60 percent. And it is on the right curve that we want to move through the end of the year. At that point, we will look at the POAMs that are generated, we will go back into those accreditations and do an IV&V, and we will reassess it. It will be an annual routine that we will follow.

Chairman TOM DAVIS. Let me ask Mr. Hughes and Mr. Wiesner, your agency systems have to connect with State systems that are not covered by FISMA for information sharing purposes. How do you ensure that your information systems are adequately protected under those circumstances?

Mr. HUGHES. That is a good question. We have agreements with States and different agencies. We have security procedures and policies that they have to agree to. We have MOUs of these agreements. And we monitor these data exchanges that go between the States and the Federal Government.

Chairman TOM DAVIS. All right.

Ms. Watson.

Ms. WATSON. I want to highly commend Mr. Hughes, U.S. Social Security Administration, and Mr. Wiesner, U.S. Department of Labor, for the fact that using the criteria that the committee used, the number of points assigned to each response is proportional to the extent the element has been implemented. You received an A+. And you started from probably lower grades, but you showed your ability to focus like a laser beam and to make the improvements along the way.

Going to Mr. Lentz and Mr. Charbo, U.S. Department of Defense defending our country, and U.S. Department of Homeland Security securing our country, you started in year 2005 with an F grade and, at the end of year 2005, you still have an F grade. Can either

one of you gentlemen explain to me why? And listening to your reports, it looks like you are just moving along and making progress. But the criteria that the committee used was a methodology that was standardized, and you came up, started with an F, and you are still at an F.

Let me know why that is the case. Mr. Lentz, let me start with you.

Mr. LENTZ. Well, ma'am, I agree that the challenges that we have in this very large organization will sometimes make the process that we use in terms of assessing our operational status one that creates the kind of assessments that one has to look very hard at, and that is what our leadership is doing every single day. And we take——

Ms. WATSON. Let me just stop you. Mr. Lentz, 5 years? Your leadership? Five years and you don't improve based on the methodology that is standardized? The way they judged every single—and I can read off all the departments. Agency for International Development, A+, starting from much lower grades before. Department of Labor, A+. Social Security, A+. Office of Personnel Management, A+. Environmental Protection Agency, A+. National Science Foundation, A.

What is happening with the two most strategic and sensitive agencies? What is it? Is there incompetence? Is there cronyism? You know, I don't feel comfortable with my Department of Defense, based on what I see here. I don't feel comfortable that my homeland is secure. And I can take a lesson from September 11th. The perpetrators were sent—the flight school, as I understand, sent them their authority to take flight lessons after September 11th. Something went wrong along the way.

Now, if you had a department, a business that made nails, and you put the metal in at the beginning of the process and, at the end, the nails came out bent, you would stop the whole operation and work backward to find out why those nails are being bent. What is happening with the Department of Defense and Homeland Security that in 5 years, based on the methodology used, you show no improvement? You tell us that the report—I guess the preceding 5 months will look better, but I am wondering what happened in those 5 years. Can you help me understand this?

Mr. LENTZ. Well, I think when we look at, when we open up our report and look at it gradually—and, as indicated in my testimony, I think we have shown some clear improvements in all the areas that FISMA is asking for. And on top of that——

Ms. WATSON. As of when? Can you help me?

Mr. LENTZ. As of starting last year and the year before.

Ms. WATSON. Well, why is it—maybe the staff is incompetent, because they graded you. I did not. The committee staff. And maybe I should ask this of the chair. You know, they score by a point. And I probably need to give this to you. And, you know, if you score within a certain range, they assign you a certain letter. And the scores were so low with the Department of Defense and Homeland Security that it resulted in an F. Now, maybe the math is all off.

I am trying to be fair. I am trying to understand what is going on with my Department of Defense that you come and you ask us—you know, we have a supplement on the floor asking us for billions

of dollars. And, you know, what are you securing, Iraq? Department of Homeland Security, what are you securing?

You know, and the grade is still coming out F. I need to understand this so when I go back to my 650,000 constituents that pay taxes, and I—I didn't vote for it, and I am not going to—I can tell them, yeah, we need to vote for this because our Department of Defense says they need this so we can win the war 10,000 miles away. We are not winning the war here. We can't even pick up the rubble down in New Orleans.

So you have to prove to me that you are doing something that will secure us as a people and secure our country. And I don't see it. So I am asking for you to educate me, to enlighten me, so I can go back and tell my constituents why I would vote to use their taxpayer dollars to defend against Iraq—which apparently is no threat to us here, but certainly a threat to life and limb over there. Give me some information, please, that there is some competence in this organization that I can take back to my constituents.

Mr. LENTZ. In looking at the grading that we have recently seen, there were two assessments that were done, one by the CIO and one by the IG, in the assessment column. The Department of Defense got a score of 85 under the CIO column. And when you look at that holistically and combine that with all the other security measures that were undertaken, such as, as the chairman indicated earlier, identity protection and management using PKI and other methods that we are, I would say that I think our security posture has significantly improved. But at the same time, I must admit, we always in this very dynamic environment that we live in, we have to constantly seek for better improvement in these areas.

Ms. WATSON. Let me address the chair. From the response I just received, is there something wrong with this scoring? Because as I look at the information provided to us on the assignment of grades, it says 0 points for a response indicating the percentage that falls below an acceptable threshold. And they give us an example: 50 percent or less known IT security weaknesses being incorporated in the plan of action. That means that you fell below the 50 percent level.

Now, if this is the methodology——

Chairman TOM DAVIS. Well, the methodology is very simple. The CIO scores and the IG scores, and when you are in doubt, GAO takes the IG score. CIO score is like when you are grading your own paper, to some extent. So in those cases, the GAO, who really gives us the numbers on which we base the grade, goes with the IG score.

Ms. WATSON. So I still haven't heard adequate response to my concerns. And I just think there is something wrong in the process. And I would advise the two of you to take the message back from me individually that the Department of Defense, the Department of Homeland Security needs to get about the business of improving the process of securing our land and our people. From what I see, and this is information that the staff gives us, I did not do the research and the evaluation and the assignment myself. You need to know that. I can only go on the information that our professional staff gives us.

I would hope the two of you, next time you come, not insult my intelligence. Otherwise, I have to question the competence of staff. But you can't tell me it is working well and the staff gave you and F, and for the last 5 years it has been F. So take that message back to the Secretaries. And Mr. Chertoff has not returned my call. When I was asking him to stop the evictions of 10,000 people, I never got a return call. So he would get an F- from me in terms of being effective just answering a call from a Congress person concerned about making—so I have no trust that it is going to get any better. Now, that is my opinion. I am speaking for myself. And you can take that message back.

Thank you, Mr. Chairman, for the time.

Chairman TOM DAVIS. Thank you very much. I would leave on that high note here, but I think that I will just ask a couple of other questions.

We asked the first panel, and I guess in fairness to DHS and DOD, do you think there are issues that arise at the larger agencies that the smaller ones don't have to contend with? I think that has been—we talked about that in our opening statement and I will give you an opportunity to comment on that again.

Mr. CHARBO. From DHS's perspective, I think there is a complexity with dealing with lots of large agencies that we have components that we have. That still doesn't change the fact when we looked at our security posture coming into the Department, where we were was not where we wanted to be in terms of our security scores and our FISMA compliance. So we have launched an aggressive project. I see good response coming from those components even though it is large, it is complex. Currently we have the data. We have good progression moving—I see good response coming from those large components, as difficult as it is.

I think the GAO had some good comments in the first panel dealing with direct appropriations, and it is difficult to get them to respond. But I would like to have a chance to execute our plan this year. And the plan that we had last year isn't the one we are currently working under.

Chairman TOM DAVIS. I mean, you are both large organizations but you are very important organizations in terms of vulnerability and where someone who has malice aforethought may be looking. So that is why we focus in on you and I think that is why Ms. Watson is just saying to DOD and Homeland Security these are two agencies that are showing up as more vulnerable than other agencies, and obviously we are alarmed. But we understand there is a lot of complexity. I know in the case of DHS we have cobbled together these different units and you are as strong as your weakest unit, to some extent, the way this works.

Mr. Lentz, would you—I will give you an opportunity to comment.

Mr. LENTZ. Yes, I completely agree that the complexity of the organization, the dynamics of moving forces—when you deploy ships out to sea, you are changing the network configurations constantly, you are deploying troops overseas, you are creating new network on the fly in global environments and high-risk environments. Clearly in a situation like that, it does represent a lot of new challenges and challenges that we take very seriously.

Chairman TOM DAVIS. OK. Anything you would like to add?

Mr. HUGHES. I would just say that we know our mission, so perhaps—we are a large organization, we have 120,000 work stations, but our mission is clear in terms of our complexity. We know the way we serve our citizens. So I don't think we have absorbed the complexity of an organization like DHS.

Chairman TOM DAVIS. OK.

Mr. WIESNER. I agree also. We have been an organization around for many, many years, and perhaps that helps out a little bit in terms of absorbing a lot of complexity in a large-scale organization like DHS.

Chairman TOM DAVIS. Well, of course this committee wrote FISMA. We don't have all the enforcement mechanisms we like, but you have heard Ms. Evans talk about that is something that they take into account as they are putting their budgets together. We are trying to coordinate appropriately with the Appropriations Committee so it is taken into account as they put their budgets together. You can fight the resources department within your own agencies. I am not asking you to come here and put you on the spot and saying are you getting enough resources with your own agency. But we understand. I mean, I understand the issues of this. And we are going to continue to push to give you the resources you need to get the job done.

I just want to congratulate those of you that have shown great improvement. And for the others, we will keep trying. I know you have plans to address this. We look forward to seeing you up here again.

Thank you very much.

[Whereupon, at 1:41 p.m., the committee was adjourned.]

[The prepared statement of Hon. Henry A. Waxman and additional information submitted for the hearing record follow:]

Statement of Rep. Henry A. Waxman, Ranking Minority Member
Committee on Government Reform
Hearing on "Leave No Computer System Behind: A Review of the 2006 Federal Computer Security Scorecards"

March 16, 2006

Thank you, Mr. Chairman. I am pleased that the Committee is holding this hearing today to examine ways that federal agencies can improve the state of federal information security.

Weaknesses in information security threaten both the ability of federal programs to operate and the privacy of citizens whose personal information is maintained in government systems. That is why Congress enacted the Federal Information Security Management Act four years ago to require agencies to address the threats to security and privacy.

The Act is designed to promote sound information security practices in federal agencies. The Act sets forth rigorous security requirements, but allows agencies flexibility in developing practices to meet these requirements in a way that fits their mission and organization.

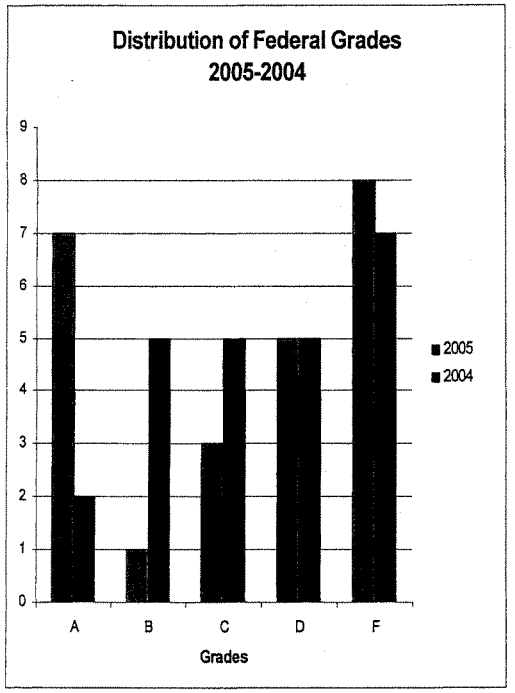
The reports from the Office of Management and Budget and the Government Accountability Office show that many agencies are making some progress in securing their systems. But over four years after 9-11, far too many weaknesses remain.

Chairman Tom Davis has graded each agency's performance in a computer security scorecard. The overall grade is an abysmal D+, the same as last year. For every agency that has taken a step forward in its security, another has taken a step backward.

I am particularly concerned about the challenges that the Department of Homeland Security and Department of Defense face in protecting the government's most critical systems and most sensitive data. Regrettably, both of these agencies continue to fare poorly on the Committee's report card.

It is possible for large agencies with aging systems and vast amounts of sensitive data to comply with FISMA. The A+ grade of the Social Security Administration proves it. I hope today we learn how SSA and the other A+ agencies have achieved their success, so their practices can be implemented in other agencies.

I look forward to the hearing and thank the witnesses for their appearance before us.



SIXTH
REPORT CARD
On
COMPUTER SECURITY
At
Federal Departments and Agencies

Overall Grade: D+

MARCH 16, 2006

FEDERAL COMPUTER SECURITY REPORT CARD			March 16, 2006		
GOVERNMENTWIDE GRADE 2005: D+					
	2005	2004		2005	2004
AGENCY FOR INTERNATIONAL DEVELOPMENT	A+	A+	DEPARTMENT OF COMMERCE	D+	F
DEPARTMENT OF LABOR	A+	B-	DEPARTMENT OF JUSTICE	D	B-
SOCIAL SECURITY ADMINISTRATION	A+	B	NUCLEAR REGULATORY COMMISSION	D-	B+
OFFICE OF PERSONNEL MANAGEMENT	A+	C-	DEPARTMENT OF TREASURY	D-	D+
ENVIRONMENTAL PROTECTION AGENCY	A+	B	DEPARTMENT OF ENERGY	F	F
NATIONAL SCIENCE FOUNDATION	A	C+	DEPARTMENT OF VETERANS AFAIRS	F	F
GENERAL SERVICES ADMINISTRATION	A-	C+	DEPARTMENT OF HEALTH AND HUMAN SERVICES	F	F
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	B-	D-	DEPARTMENT OF THE INTERIOR	F	C+
SMALL BUSINESS ADMINISTRATION	C+	D-	DEPARTMENT OF DEFENSE	F	D
DEPARTMENT OF TRANSPORTATION	C-	A-	DEPARTMENT OF STATE	F	D+
DEPARTMENT OF EDUCATION	C-	C	DEPARTMENT OF HOMELAND SECURITY	F	F
HOUSING AND URBAN DEVELOPMENT	D+	F	DEPARTMENT OF AGRICULTURE	F	F

Prepared by the Government Reform Committee, chaired by Tom Davis, based on reports required by the Federal Information Security Management Act of 2002.

Federal Computer Security Grades
2001-2005

Agency	2005 Score	2005 Grade	2004 Score	2004 Grade	2003 Score	2003 Grade	2002 Score	2002 Grade	2001 Score	2001 Grade
Agriculture	24	F	49.5	F	40	F	36	F	31	F
AID	100	A+	99	A+	70.5	C-	52	F	22	F
Commerce	67	D+	56.5	F	72.5	C-	68	D+	51	F
DOD**	38.75	F	65	D	65.5	D	38	F	40	F
Education	71	C-	76.5	C	77	C+	66	D	33	F
Energy	46.75	F	48.5	F	59.5	F	41	F	51	F
EPA	97.5	A+	84	B	74.5	C	63	D-	69	D+
GSA	92.5	A-	79.5	C+	65	D	64	D	66	D
HHS	45.5	F	49.5	F	54	F	61	D-	43	F
DHS	33.5	F	20.5	F	34	F	--	--	--	--
HUD	67.5	D+	28	F	40	F	48	F	66	D
Interior	41.5	F	77	C+	43	F	37	F	48	F
Justice	66.5	F	82.5	B-	55.5	F	56	F	50	F
Labor	99	A+	83	B-	86.5	B	79	C+	56	F
NASA	80	B-	60	D-	60.5	D-	68	D+	70	C-
NRC	60.5	D-	88	B+	94.5	A	74	C	34	F
NSF	95	A	77.5	C+	90.5	A-	63	D-	87	B+
OPM	98	A+	72.5	C-	61.5	D-	52	F	39	F
SBA	78	C+	60	D-	71	C-	48	F	48	F
SSA	99	A+	86	B	88	B+	82	B-	79	C+
State	37.5	F	69.5	D+	39.5	F	54	F	69	D+
Transportation	71.5	C-	91.5	A-	69	D+	28	F	48	F
Treasury**	60.5	D-	68	D+	64	D	48	F	54	F
VA**	46	F	50	F	76.5	C	50	F	44	F
Government-wide Average	**67.4**	**D+**	**67.3**	**D+**	**65**	**D**	**55**	**F**	**53**	**F**

****The Inspector General for these agencies did not provide independent evaluations of their agencies' FISMA reports for FY03. Therefore these scores are based on self-reported numbers submitted by these agencies.**

How Grades Were Assigned

The Committee's computer security grades are based on information contained in agencies' and Inspectors General's (IGs) Federal Information Security Management Act (FISMA) reports to the Office of Management and Budget (OMB) for fiscal year 2005.

On December 17, 2002, the President signed into law the Electronic Government Act. Title III of that Act is the FISMA. FISMA lays out the framework for annual IT security reviews, reporting and remediation planning at federal agencies. FISMA requires that agency heads and IGs evaluate their agencies' computer security programs and report the results of those evaluations to OMB in September of each year along with their budget submissions. FISMA also requires that agency heads report the results of those evaluations annually to the Congress and the Government Accountability Office.

OMB's 2005 reporting guidance instructed the agencies and IGs to submit reports summarizing the results of annual IT security reviews of systems and programs, agency progress on correcting identified weaknesses, and the results of other work performed during the reporting period. Agencies and IGs were required to use OMB's performance measures in assessing and reporting the status of their agencies' security programs. In addition, agencies were permitted to include additional performance measures they had developed.

Assignment of Grades

In assigning grades, the Committee followed the methodology developed for the fiscal year 2004 FISMA grades, with the exception of adjustments required by changes in OMB's FISMA reporting instructions (see below). This approach ensures consistency in the methodology used to assign grades and serves to highlight progress made by an agency if this year's grade indicates improvement.

The weighted scores are based on OMB's performance metrics, with a perfect score totaling 100 points. OMB provided a range of responses for most questions. The number of points assigned to each response is proportional to the extent the element has been implemented. For example, agencies received zero (0) points for a response indicating a percentage that falls below an acceptable threshold (for example: 50% or less of known IT security weaknesses being incorporated in the Plan of Action and Milestones). Proportionally, more points were given for answers that ranged between 51 and 70%, 81 and 95%, etc. The full weighted value was awarded for answers that ranged between 96 and 100%.

For more specific weighting of questions see the scoring methodology.

The Committee tallied the scores for the 24 agencies on the basis of its analysis of agency and IG responses. The final numerical score is the basis for the agency's letter grade. Letter grades for the 24 major departments and agencies were assigned as follows:

90 to 93 = A-	94 to 96 = A	97 to 100 = A+
80 to 83 = B-	84 to 86 = B	87 to 89 = B+
70 to 73 = C-	74 to 76 = C	77 to 79 = C+
60 to 63 = D-	64 to 66 = D	67 to 69 = D+
59 and lower = F		

Major Changes to the Weighting of Grades

Changes in OMB's FISMA reporting instructions from FY04 to FY05 required the Committee to make several adjustments to the scoring methodology that was used to determine the FISMA grades. The major changes are listed below.

To facilitate future consistency, the Committee continued using the following major categories: Annual Testing, Plan of Action and Milestones, Certification and Accreditation, Configuration Management, Incident Detection and Response, Training and Systems Inventory. Changes for each area are listed below.

Annual Testing – Removed questions regarding the CIO and NIST self-assessment that are not included in OMB's FY05 FISMA reporting guidance. Expanded questions regarding the review of agency and contractor systems, to include impact levels. Added question regarding IGs' evaluation of the agency's oversight. If an IG indicates a range of 96 to 100%, no points are taken; if between 51 and 95 % the agency loses half of its annual testing points; if 50% or less, the agency loses all annual testing points.

Plan of Action and Milestones – Removed agency-related POA&M question since it is not in FY05 FISMA reporting guidance. All POA&M questions for FY05 FISMA reporting were directed to the IG.

Certification and Accreditation – Removed question relating to security controls being integrated into the life cycle, as this issue is no longer a reporting requirement. Expanded questions to include impact levels—high, moderate, low.

Configuration Management – Removed the question regarding the patching of security vulnerabilities and added a question regarding emerging technologies.

Incident Response and Detection – Removed the question regarding systems undergoing vulnerability scans and penetration tests.

Training – No changes made.

Inventory – Removed agency-related inventory question and added two new IG questions for a total of three questions. The IG must rate the agency at 96% to 100% for all three questions or a full letter grade will be deducted from the final score.

Improvements still Needed

Although many agencies reported improvements in their implementation of FISMA, such as certifying and accrediting a higher percentage of their systems and maintaining an inventory, much work is still needed to ensure federal information systems are secure. Areas of continued weaknesses include:

- Annual Testing
    a. Some agencies reported large numbers of their systems as uncategorized. These agencies coincidentally all scored in the F range.
    b. While many agencies show improvements over last year in testing their contingency plans, several report testing under 60% of contingency plans for high-impact systems.
- Configuration Management
  Many agencies have begun to develop or have these policies; however, several agencies continue to have a low level of implementation.
- Incident Reporting
  Agencies continued to show inconsistencies in reporting incidents. Some agencies reported few or no incidents. Several reported less than half of all incidents to USCERT.
- Training
  Most agencies have ensured that their employees have received security training and awareness; however, agencies are less successful in ensuring that those with significant security responsibilities receive specialized training.
- Inventory
  Many agencies have not developed an inventory of major IT systems.
- Overall
  Four of the largest agencies have failing scores: Treasury, DOD, DHS, USDA.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

May 5, 2006

The Honorable Tom Davis
Chairman
Government Reform Committee
U.S. House of Representatives
2348 Rayburn House Office Building
Washington, DC 20515-4611

Dear Chairman Davis:

Thank you very much for the opportunity to testify before the Government Reform Committee on the subject of Federal Computer Security Scorecards on March 16, 2006. Your interest and partnership on this issue are very much appreciated.

In response to the Committee's computer security scorecard hearing, enclosed you will find my answers to your questions for the record. I look forward to a continued partnership with you in pursuit of robust computer security in the Federal Government. Thank you again for all of your efforts.

If you or your staff have any questions, please do not hesitate to call me at (202)395-1181.

Sincerely,

Karen S. Evans, Administrator
Office of Electronic Government and
Information Technology

Karen Evans/Congressman Davis
QFRs regarding breach notification

You asked the following questions:

Do federal agencies notify citizens when a breach of personally identifiable information occurs on government databases?

What, if any, guidelines exist to determine if a breach requires notification?

Consistent with the policies and objectives underlying existing privacy protection statutes and requirements, several agencies have developed formal directives for providing notice in the event of unauthorized release or access to identifiable information in federal information technology systems. Generally speaking, agencies address actual or potential compromises of information on a case-by-case basis, determining whether to notify record subjects after considering, among other criteria, the magnitude of potential harm and the sensitivity and significance of information compromised or potentially compromised.

For example, in the event of unauthorized access to or disclosure of personally identifiable information from a system of records, some agencies -- as part of their implementation of the safeguard requirement in Section e(10) of the Privacy Act -- provide administrative notice to the individual when unauthorized access or disclosure might result in substantial harm, embarrassment, inconvenience or unfairness to the individual.

Another example is the Privacy and Security Rules implemented pursuant to the Health Insurance Portability and Accountability Act (HIPAA) impose on covered entities (including federal agencies administering health information) a duty to mitigate harm resulting from an unauthorized use or disclosure of protected health information ("A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate."). This requirement does not prescribe what mitigation procedures must be implemented, only that the entity "mitigate harm." OMB's understanding is that components within VA, HHS and DOD that administer health care programs have developed notification procedures pursuant to the Rules.

In addition, when involving information technology specifically, the Federal Information Security Management Act (FISMA) requires agencies to develop and implement procedures to detect, report, and respond to security incidents and mitigate risks before substantial harm occurs. FISMA further requires agencies to notify the Federal incident handling center, law enforcement offices, and agency Inspectors General when significant incidents occur. With respect to the issue of the circumstances in which (and, in such circumstances, when) individuals should be notified that the security of information about them may have been compromised, law enforcement and national security equities may bear upon the resolution of this issue, as public notification of a data breach without proper coordination could frustrate an ongoing investigation into the source of the data breach. Any reporting requirements in this area should take such interests into account.

Finally, the Attorney General's Guidelines for Victim and Witness Assistance (May 2005) address the circumstances in which crime victims must be notified of criminal acts affecting them.

OMB and the agencies recognize the potential for harm caused by unauthorized access to or disclosure of personally identifiable information. OMB has begun working with the agencies to explore the pertinent considerations and appropriate next steps in the area of breach notification.