AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

NO COMPUTER SYSTEM LEFT BEHIND: A REVIEW OF THE FEDERAL GOVERNMENT'S D+ INFORMATION SECURITY GRADE

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

APRIL 7, 2005

Serial No. 109–13

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

20–562 PDF WASHINGTON : 2005

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

COMMITTEE ON 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
GINNY BROWN-WAITE, Florida
JON C. PORTER, Nevada
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. MCHENRY, North Carolina
CHARLES W. DENT, Pennsylvania
VIRGINIA FOXX, North Carolina

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)

MELISSA WOJCIAK, *Staff Director*
DAVID MARIN, *Deputy Staff Director/Communications Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

CONTENTS

	Page
Hearing held on April 7, 2005	1
Statement of:	
Crandlemire, Bruce N., Assistant Inspector General for Audit, U.S. Agency for International Development; John Streufert, Acting Chief Information Officer, U.S. Agency for International Development, accompanied by Mark Norman, USAID OIG; Melinda Dempsey, USAID OIG; Philip M. Heneghan, USAID; Frank Deffer, Assistant Inspector General for Information Technology, U.S. Department of Homeland Security; Steve Cooper, Chief Information Officer, U.S. Department of Homeland Security, accompanied by Edward G. Coleman, DHS OIG; Ted Alves, Assistant Inspector General for IT and Financial Management, U.S. Department of Transportation; Daniel Matthews, Chief Information Officer, U.S. Department of Transportation, accompanied by Rebecca Leng, DOT OIG; Ed Densmore, DOT OIG; Nate Custer, DOT OIG; Vicki Lord, DOT OCIO; and Dr. Dan Mehan, CIO, FAA	71
Alves, Ted	105
Cooper, Steve	99
Crandlemire, Bruce N.	71
Deffer, Frank	89
Matthews, Daniel	124
Streufert, John	79
Wilshusen, Greg, Director, Information Security Issues, U.S. Government Accountability Office; and Karen S. Evans, Administrator, Office of E-Government and Information Technology, U.S. Office of Management and Budget	22
Evans, Karen S.	52
Wilshusen, Greg	22
Letters, statements, etc., submitted for the record by:	
Alves, Ted, Assistant Inspector General for IT and Financial Management, U.S. Department of Transportation, prepared statement of	107
Cooper, Steve, Chief Information Officer, U.S. Department of Homeland Security, prepared statement of	102
Crandlemire, Bruce N., Assistant Inspector General for Audit, U.S. Agency for International Development, prepared statement of	74
Cummings, Hon. Elijah E., a Representative in Congress from the State of Maryland, prepared statement of	17
Davis, Chairman Tom, a Representative in Congress from the State of Virginia, prepared statement of	4
Deffer, Frank, Assistant Inspector General for Information Technology, U.S. Department of Homeland Security, prepared statement of	91
Evans, Karen S., Administrator, Office of E-Government and Information Technology, U.S. Office of Management and Budget, prepared statement of	54
Matthews, Daniel, Chief Information Officer, U.S. Department of Transportation, prepared statement of	126
Ruppersberger, Hon. C.A. Dutch, a Representative in Congress from the State of Maryland, prepared statement of	12
Streufert, John, Acting Chief Information Officer, U.S. Agency for International Development, prepared statement of	81
Wilshusen, Greg, Director, Information Security Issues, U.S. Government Accountability Office, prepared statement of	24

NO COMPUTER SYSTEM LEFT BEHIND: A REVIEW OF THE FEDERAL GOVERNMENT'S D+ INFORMATION SECURITY GRADE

THURSDAY, APRIL 7, 2005

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

The committee met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Tom Davis (chairman of the committee) presiding.

Present: Representatives Davis, Duncan, Cummings, Ruppersberger, and Norton.

Staff present: Ellen Brown, legislative director and senior policy counsel; Robert Borden, counsel/parliamentarian; Rob White, press secretary; Victoria Proctor, senior professional staff member; Jamie Hjort, professional staff member; Chaz Phillips, policy counsel; Teresa Austin, chief clerk; Sarah D'Orsie, deputy clerk; Kristin Amerling, minority deputy chief counsel; Karen Lightfoot, minority communications director/senior policy advisor; Nancy Scola, minority professional staff member; Earley Green, minority chief clerk; and Jean Gosa, minority assistant clerk.

Chairman TOM DAVIS. Good morning. The committee will come to order.

I would like to welcome everyone to today's hearing on implementation of FISMA, the Federal Information Security Management Act of 2002.

We rely heavily on information technology and the Internet to support our economy, our national security and government operations. For instance, e-commerce is more popular than ever; Christmas 2004 saw record high consumer demapped on retail Web sites. IT systems are used to operate and protect our critical infrastructures. And in the Federal Government, electronic government initiatives create efficiencies, save taxpayers time and money, and help eliminate redundant processes.

Given the interconnectivity of systems, all it takes is one weak link to break the chain. All users, whether they are at home or at school or at work, need to understand the impact of weak security and the measures that should be taken to prevent cyber attacks.

Everyone must protect his or her cyberspace, and of course, that includes the government. Therefore, it is critical that the Federal Government adequately protect its systems to ensure the continuity of operations, and to maintain public trust. This is particularly true of agencies such as the Internal Revenue Service, the Social

Security Administration and the Department of Veterans Affairs that maintain citizens' personal information in their systems. Recent failures by the Bank of America and Choice Point have focused the spotlight on identity theft. Successful FISMA implementation is important because a similar event could occur in the government.

Like the private sector, agencies are not immune to the loss of personal information. Threats to government systems could result in identity theft and subsequent financial damage and frustration, as well as diminished trust in government IT capabilities and electronic government programs.

Every day Federal information systems are subjected to probes or attacks from outside sources. Cyber attacks are evolving and becoming more sophisticated. Therefore, a government information security management program must be comprehensive, yet flexible enough to adapt to the changing cyber threat environment. It is a matter of good management and good business practice, but it is also a matter of national security. FISMA provides that structure by requiring that each agency create a comprehensive risk-based approach to agency-wide information security management.

OMB performs an important role in the information security management process by encouraging agencies to adopt a new approach to security. In the past, information security was often seen as an afterthought, more of a crisis response than a management tool. OMB is helping to alter that perspective. It holds the agencies responsible for protecting Federal systems through business case evaluations so that agencies can better fulfill their missions. OMB requires agencies to address their security deficiencies before they are permitted to spend money on IT upgrades or new IT projects.

I support this action because it forces agencies to concentrate on security before adding new layers of systems to their architecture and potentially complicating their security concerns.

I'm also pleased that OMB has identified a sixth line of business, cyber security. Laws like FISMA and the Clinger-Cohen amendment require every agency to think about and invest in information security. However, each agency does it differently. The reason FISMA grades show the Federal Government still has a long way to go when it comes to information security. As with the other five lines of business, the goal of the cyber security line of businesses is to use business principles and best practices to identify common solutions for business processes and/or technology-based shared services for government agencies. The intended result is better, more efficient and consistent security across the Federal Government for the same amount of dollars, if not less. And at the end of the day, it's not how much money you spend, though, it's how well you spend it.

To help us gauge the agencies information security progress, FISMA requires the CIOs and IGs to submit reports to Congress and OMB. The committee enlists GAO's technical assistance to prepare the annual scorecard. This year the government made a slight improvement, receiving a D+. The overall government score is two points above last year, but needless to say, this isn't impressive. Progress is slow. Our objective today is to find out how the govern-

ment can improve, and why some agencies can show remarkable improvement while others appear to flounder.

We will hear from the IGs and CIOs of two agencies that improved their scores this year, Department of Transportation and the U.S. Agency for International Development. We will also hear from the IG and the CIO of the Department of Homeland Security, a poor performer again this year. I think it is worth noting that DHS has cyber security responsibilities for the Nation, and must work with the private sector regularly on these issues. Given this role, DHS needs to have its house in order and should become a security leader among agencies. What is holding them up? Well, the DHS witnesses will discuss the unique challenges that they face in a large and relatively new agency, and what actions they are taking to improve their information security, giving us a better understanding of their difficulties.

In addition, we're concerned about how well the CIO and IG offices communicate about issues such as their interpretations of the OMB reporting requirements. Disagreements on interpretation may impact their respective reports and make it difficult for us to get an accurate picture of the agency's information security progress. This also raises questions about the clarity of the guidance, and whether agencies respond to OMB about the guidance during the comment period so their comments and concerns are adequately addressed in the final version.

We will examine whether the IGs need a standardized information security audit framework similar to that used for financial management systems. Also, we need to address whether agencies need additional guidance, procedures or resources to improve their information security and fully comply with FISMA.

Panel one witnesses from GAO and OMB will focus on information security from the government-wide perspective. Panel two is comprised of agency representatives and will focus on the agency-level perspective on implementation of FISMA.

We'll hear from the IGs and CIOs at USAID, DHS, and the Department of Transportation. GAO will join panel two for the question-and-answer period.

[The prepared statement of Chairman Tom Davis follows:]

Oversight Hearing

"No Computer System Left Behind: A Review of the Federal Government's D+ Information Security Grade"

Thursday, April 7, 2005
10:00 a.m.
Room 2154 Rayburn House Office Building

Opening Statement

Good morning. A quorum being present, the Committee on Government Reform will come to order. I would like to welcome everyone to today's hearing on the implementation of FISMA, the Federal Information Security Management Act of 2002.

We rely heavily on information technology and the Internet to support our economy, national security, and government operations. For instance, e-commerce is more popular than ever – Christmas 2004 saw record high consumer demand on retail websites. IT systems are used to operate and protect our critical infrastructures. And in the federal government, electronic government initiatives create efficiencies, save taxpayers time and money, and help eliminate redundant processes.

Given the interconnectivity of systems, all it takes is one weak link to break the chain. All users – whether they are at home,

school, or work – need to understand the impact of weak security and the measures that should be taken to prevent or respond to cyber attacks.

Everyone must protect his or her piece of cyberspace – that includes the government. Therefore, it is critical that the federal government adequately protect its systems to ensure the continuity of operations and to maintain public trust. This is particularly true of agencies such as the Internal Revenue Service, the Social Security Administration, and the Department of Veterans Affairs that maintain citizens' personal information in their systems. Recent failures have focused the spotlight on identity theft. Successful FISMA implementation is important because a similar event could occur in the government. Like the private sector, agencies are not immune to the loss of personal information. Threats to government systems could result in identity theft and subsequent financial damage and frustration, as well as diminished trust in government IT capabilities and electronic government programs.

Everyday, federal information systems are subjected to probes or attacks from outside sources. Cyber attacks are evolving and becoming more sophisticated. Therefore, a

government information security management program must be comprehensive, yet flexible enough to adapt to the changing cyber threat environment. It is a matter of good management and good business practice, but it's also a matter of national security. FISMA provides that structure, by requiring each agency to create a comprehensive risk-based approach to agency-wide information security management.

OMB performs an important role in the information security management process by encouraging agencies to adopt a new approach to security. In the past, information security was often seen as an afterthought – more of a crisis response than a management tool. OMB is helping to alter that perspective. It holds the agencies responsible for protecting federal systems through business case evaluations so that agencies can better fulfill their missions. OMB requires agencies to address their security deficiencies before they are permitted to spend money on IT upgrades or new IT projects. I support this action because it forces agencies to concentrate on security before adding new layers of systems to their architecture and potentially complicating their security concerns.

I am also pleased that OMB has identified a sixth line of business – cyber security. Laws like FISMA and the Clinger-Cohen amendment require every agency to think about and invest in information security. However, each agency does it differently. The recent FISMA grades show the Federal government still has a long way to go when it comes to information security. As with the other five lines of business, the goal of the cyber security line of business is to use business principles and best practices to identify common solutions for business processes and/or technology-based shared services for government agencies. The intended result is better, more efficient and consistent security across the Federal government for the same amount of dollars, if not less. At the end of the day, it's not how much money you spend, but how well you spend it.

To help us gauge the agencies information security progress, FISMA requires the CIOs and IGs to submit reports to Congress and OMB. The committee enlists GAO's technical assistance to prepare the annual scorecard. This year the government made a slight improvement, receiving a D+. The overall government score is two points above last year. Needless to say, this is not impressive. Progress is slow. Our objective today is to find out

how the government can improve and why some agencies can show remarkable improvement while others appear to flounder.

We will hear from the IGs and CIOs of two agencies that improved their scores this year – the Department of Transportation and the US Agency for International Development. We will also hear from the IG and CIO at the Department of Homeland Security – a poor performer again this year. I think it is worth noting that DHS has cyber security responsibilities for the nation and must work with the private sector regularly on these issues. Given this role, DHS must have its house in order and should become a security leader among agencies. What's holding them up? The DHS witnesses will discuss the unique challenges they face in a large and relatively new agency, and what actions they are taking to improve their information security.

In addition, we are concerned about how well the CIO and IG offices communicate about issues such as their interpretations of the OMB reporting requirements. Disagreements on interpretation may impact their respective reports and make it difficult for us to get an accurate picture of the agency's information security progress. This also raises questions about the clarity of the guidance and whether agencies respond to OMB about the

guidance during the comment period so their comments and concerns may be addressed in the final version.

We will examine whether the IGs need a standardized information security audit framework similar to that used for financial management systems. Also we will address whether agencies need additional guidance, procedures, or resources to improve their information security and fully comply with FISMA.

Panel One witnesses from GAO and OMB will focus on information security from the government-wide perspective. Panel Two is comprised of agency representatives and will focus on the agency-level perspective on implementation of FISMA. We'll hear from the IGs and CIOs at USAID, DHS, and the Department of Transportation. GAO will join Panel Two for the question and answer period.

Chairman TOM DAVIS. I now recognize our distinguished ranking member, Mr. Waxman, for his opening statement.

Mr. RUPPERSBERGER. I'm not Mr. Waxman, I'm a little bit larger than Mr. Waxman.

Chairman TOM DAVIS. Well, when he comes, we will recognize him. In the meantime, we're very pleased to recognize from Baltimore City, Mr. Ruppersberger, who I will be happy to recognize.

Mr. RUPPERSBERGER. Well, first, thank you for calling this hearing today on OMB's report to Congress on the Federal Information Security Management Act.

According to the report, the U.S. Agency for International Development and the Department of Transportation received the highest grades of all 24 agencies reviewed. I hope that during today's hearing, we will be able to pull out some best practicing and tangible suggestions from those agencies as to how the other 22 can improve their grades. It is disappointing and unacceptable that our government agencies' overall grade is a D+, however, I'm encouraged by the few successes that will be discussed here today.

The F grade for the Department of Homeland Security is totally unacceptable because of the high stakes involved and their mission to protect our national security. Last week, the President's Commission on the Intelligence Capabilities of the United States issued their report regarding WMDs. In the report's postscript the Commission identified security, counterintelligence, and information assurance as crucial issues in the intelligence community and the Director of National Intelligence in the next few years to come.

The Commission acknowledges that they only scratched the surface of the problem, and the Commission recommends early action to define new strategies for managing security in the 21st century, security that includes information assurance, which is why we're all here today.

This recommendation from the Commission will be a beneficial step in the process for the Department of Homeland Security and other security offices to improve their infrastructure security and their information and cyber security efforts.

The good news is that the Justice Department improved the most, going from an F last year to a B- this year. Currently, as graded, the FBI is evaluated within the overall grade given to Justice. Based on the FBI's mission regarding national security interests, I believe they should be graded separately from the Department of Justice.

Again, according to the President's Commission, further reforms are also necessary in the FBI's information technology infrastructure which remains a persistent obstacle for successful execution of the FBI's national security mission.

If we look at the problem as a national security issue in addition to a general information security issue, I think we will be able to come together to find solutions that will work across all agencies. I know there is always a tradeoff between the cost of implementing a security measure and the potential risks if we do not. I feel that projecting our citizens and the government from information security breaches is worth the cost that will be incurred to set up appropriate security measures. I am concerned about all of these issues, but I think if we get past the grades and use this hearing

and OMB's report as a guide, I think we will be able to quickly improve information security government-wide.

We're here today to point out a problem and to see what we can do to fix it. These failing grades are unacceptable. We need to learn from those agencies who are doing well so that we can improve individual agency's scores and the government-wide score.

Thank you, Mr. Chairman.

[The prepared statement of Hon. C.A. Dutch Ruppersberger follows:]

Congressman C.A. Dutch Ruppersberger
Committee on Government Reform

"No Computer Left Behind: A Review of the Federal Government's D+ Information Security Grade"

April 7, 2005

Statement:

Thank you Mr. Chairman for calling this hearing today on OMB's report to Congress on the Federal Information Security Management Act.

According to the report the U.S. Agency for International Development and the Department of Transportation received the highest grades of all 24 agencies reviewed. I hope that during today's hearing we will be able to pull out some best practices and tangible suggestions from those agencies as to how the other 22 can improve their grades.

It is disappointing and unacceptable that our government agencies' average overall grade is a D+, however I am encouraged by the few successes that will be discussed here today.

The "F" grade for the Department of Homeland Security is totally unacceptable because of the high stakes involved and their mission to protect our national security.
Last week the President's Commission on the Intelligence Capabilities of the United States issued their report regarding WMDs. In the report's postscript the Commission identified

security, counter intelligence, and information assurance as crucial issues to the intelligence community and the Director of National Intelligence (DNI) in the next few years to come.

The Commission acknowledges that they only scratched the surface of the problem and the Commission, "recommends early action to define new strategies for managing security in the 21st century." Security that includes information assurance, which is why we are all here today.

This recommendation from the Commission can be a beneficial step in the process for DHS and other security offices to improve their infrastructure security and their information and cyber security efforts.

The good news is that the Justice Department improved the most, going from an "F" last year to a "B-" this year. Currently as graded, the FBI is evaluated within the overall grade given to Justice. Based on FBI's mission regarding national security interests, I believe they should be graded separately from the Department of Justice.

Again, according to the President's Commission, "further reforms are also necessary in the FBI's information technology infrastructure, which remains a persistent obstacle to successful execution of the FBI's national security mission."

If we look at this problem as a national security issue in addition to a general information security issue, I think we will be able to come together to find solutions that will work across all agencies.

I know there is always a trade-off between the cost of implementing a security measure and the potential risks if we do not. I feel that protecting our citizens and the government from information security breaches is worth the cost that will be incurred to set up appropriate security measures.

I am concerned about all of these issues, but I think if we get passed the "grades" and use this hearing and OMB's report as a guide, I think we will be able to quickly improve information security government-wide.

We are here today to point out a problem and to see what we can do to fix it. These failing grades are unacceptable. We need to learn from those agencies that are doing well so that we can improve the individual agencies scores and the government-wide score.

Thank you again.

Chairman TOM DAVIS. Thank you very much. I do not see Mr. Waxman, even though he is in my script.

The gentleman from Maryland, any opening statement?

Mr. CUMMINGS. Yes, thank you very much.

Mr. Chairman, I, too, thank you for calling this important hearing on the effectiveness of the Federal Government's ongoing attempt to strengthen the security and reliability of its information and information systems.

Decades ago, the necessity of such a hearing would have been questionable as information technology and the Internet were not as prevalent nor as indispensable in the Federal Government as they are today. In the 21st century, one need not look very far to see how ambiguous information technology and the Internet have become in the day-to-day operations of the Federal Government. Communications now travel as fast and as far as the Internet allows. The electronic processing of information allows delivery of services to function with unprecedented ease and accuracy. The sharing of information intergovernmentally and across sectors can permit the Federal Government to operate with renewed effectiveness.

However, with all the advantages that accompany the Federal Government's information technology capabilities, there still exist critical areas of concern. The terms "computer virus," "worm" and "hacker" are now part of the modern day lexicon for good reason. Given the sensitivity of personal and confidential data found in Federal information systems in agencies such as the Internal Revenue Service and the Department of Defense, the potential exists for cyber criminal, terrorist or foreign nation to wreak havoc.

The American people are acutely aware that such vulnerabilities could not only result in identity theft and a loss of privacy, but also endanger our economy and undermine our national security.

Due to these concerns, information security has become a top governmental priority. To that end, Congress passed the Federal Information Security Management Act [FISMA], in 2002. This legislation established a comprehensive framework to safeguard the Federal Government's information and information systems.

Agencies are mandated to implement an information security program, which includes performing risk assessments, accounting for utilized information systems, and developing procedures to ensure the accessibility and continuity of information. Agencies must also furnish the Office of Management and Budget with an annual report on the effectiveness of their program. These agency reports form the basis of the Government Reform Committee's Federal computer security report card. Specifically, the FISMA report for 2004 acknowledges some improvements and perennial challenges in this area.

It states that agencies have made substantial progress in the certification and accreditation of systems, the incorporation of built-in security costs, the annual testing of system controls, the development of contingency plans to ensure operational continuity, and the implementation of security configuration requirements. This progress is commendable, however, given that the 2004 government-wide grade for information security is a D+, information technology is too early to celebrate. Critically important agencies such

as the Department of Homeland Security, the Department of Health and Human Services and the Department of Veteran Affairs all received Fs.

I would argue no one here would be satisfied if their child brought home these grades from school. How can we afford to have a lower standard for the Federal Government? The American people demand excellence, and Cs, Ds and Fs in securing the Federal Government's information just won't do.

Today's hearing will serve as an avenue to identify what needs to occur to assist Federal agencies in realizing the goals of FISMA. I hope the witnesses will provide insight to help Congress determine whether agencies require additional guidance in order to meet FISMA requirements, the responsibilities of agency Inspectors General in this process, and the need to possibly provide increased flexibility in assessing agency compliance with FISMA mandates.

With that, Mr. Chairman, I again thank you for calling the hearing, and I yield back.

[The prepared statement of Hon. Elijah E. Cummings follows:]

Opening Statement

Elijah E. Cummings

Full Committee Hearing entitled, "No Computer System Left Behind: A Review of the Federal Government's D+ Information Security Grade"

Committee on Government Reform
U.S. House of Representatives
109th Congress

Thursday, April 7, 2005
10:00 a.m.

Room 2154 Rayburn House Office Building

Mr. Chairman, thank you for calling this important hearing on the effectiveness of the federal government's ongoing attempt to strengthen the security and reliability of its information and information systems.

Decades ago, the necessity of such a hearing would have been questionable as information technology and the Internet were not as prevalent nor as indispensable in the federal government as they are today. In the 21st Century, one need not look very far to see how ubiquitous information technology and the Internet have become in the day-to-day operations of the federal government.

Communications now travel as fast and as far as the Internet allows. The electronic processing of information allows the delivery of services to function with unprecedented ease and accuracy. The sharing of information intergovernmentally and across sectors can permit the federal government to operate with renewed effectiveness.

However, with all the advantages that accompany the federal government's information technology capabilities, there still exist critical areas of concern. The terms computer virus, worm, and hacker are now part of the modern day lexicon for good reason. Given the sensitivity of personal and confidential data found in federal information systems in agencies such as the Internal Revenue Service and the Department of Defense, the potential exists for a cyber criminal, terrorist, or foreign nation to wreak havoc.

The American people are acutely aware that such vulnerabilities could not only result in identity theft and a loss of privacy, but also endanger our economy and undermine our national security.

Due to these concerns, information security has become a top governmental priority. To that end, Congress passed the Federal Information Security Management Act (FISMA) in 2002. This legislation established a comprehensive framework to safeguard the federal government's information and information systems.

Agencies are mandated to implement an information security program, which includes performing risk assessments, accounting for utilized information systems, and developing procedures to ensure the accessibility and continuity of information. Agencies must also furnish the Office of Management and Budget with an annual report on the effectiveness of their program.

These agency reports form the basis of the Government Reform Committee's federal computer security report card. Specifically, the FISMA report for 2004 acknowledges some improvements and perennial challenges in this area. It states that agencies have made substantial progress in the certification and accreditation of systems, the incorporation of built in security costs, the annual testing of system controls, the development of contingency plans to ensure operational continuity, and the implementation of security configuration requirements.

This progress is commendable. However, given that the 2004 governmentwide grade for information security is a D+, it is too early to celebrate. Critically important agencies such as the Department of Homeland Security, the Department of Health and Human Services, and the Department of Veterans Affairs all received F's.

I would argue no one here would be satisfied if their child brought home these grades from school. How can we afford to have a lower standard for the federal government? The American people demand excellence and C's, D's and F's in securing the federal government's information just won't do.

Today's, hearing will serve as an avenue to identify what needs to occur to assist federal agencies in realizing the goals of FISMA. I hope the witnesses will provide insight to help Congress determine whether agencies require additional guidance in order to meet FISMA requirements, the responsibilities of agency Inspectors General in this process, and the need to possibly provide increased flexibility in assessing agency compliance with FISMA mandates.

Mr. Chairman, again thank you for calling this hearing and I yield back the balance of my time.

Chairman TOM DAVIS. Well, thank you very much.

For our first panel we have Greg Wilshusen, who is the Director of Information Security Issues, at the Government Accountability Office, who is no stranger to this committee. And we have Karen Evans, who is the Administrator of the Office of E-Government and Information Technology at the Office of Management and Budget. I'm not sure if this is your first time in a full committee, you have done a lot in the subcommittee, but we welcome you, we're happy to hear from you, and we appreciate the job that you are doing.

You know it is our policy to swear witnesses in, so would you rise and raise your right hands.

[Witnesses sworn.]

Chairman TOM DAVIS. Thank you very much.

STATEMENTS OF GREG WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; AND KAREN S. EVANS, ADMINISTRATOR, OFFICE OF E-GOVERNMENT AND INFORMATION TECHNOLOGY, U.S. OFFICE OF MANAGEMENT AND BUDGET

STATEMENT OF GREG WILSHUSEN

Mr. WILSHUSEN. Mr. Chairman, and members of the committee, I am pleased to be here today to discuss Federal efforts to implement requirements of the Federal Information Security Management Act of 2002 [FISMA]. This act requires each agency to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided and/or managed by another agency or contractor. Agency programs are to include eight components, such as periodic assessment of risks and periodic testing and evaluation of controls. FISMA also requires OMB, Federal agencies and Inspectors General [IGs], to report each year on efforts to implement these programs.

Mr. Chairman, my bottom-line message today is that continued efforts are needed to sustain progress made by the agencies in implementing the requirements of FISMA.

In my testimony today, I will note areas where agencies have made significant progress and those areas where challenges remain. In addition, I will discuss opportunities for improving the annual FISMA reporting process.

Our reviews of information security controls at Federal agencies have found that significant information security weaknesses continue to place a broad array of Federal operations and assets at risk of misuse and disruption. As a result, we continue to designate Federal information security as a government-wide high risk area in our recent update to GAO's high-risk series.

In its fiscal year 2004 report to the Congress, OMB noted that the 24 major Federal agencies continued to make significant progress in implementing key information security requirements. For example, OMB reported that the percentage of Federal information systems that have been certified and accredited rose 15 points to 77 percent. Systems certification and accreditation is a process by which agency officials authorize systems to operate. It

is to include a security of the management, operational and technical security controls in the system.

However, OMB, the agencies, and IGs also reported several areas where implementing effective information security practices remains a challenge. For example, seven IGs 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.

As another example, 43 percent of Federal systems did not have a tested contingency plan. These plans provide specific instructions for restoring critical systems, business processes, and information in the event of a disruption of service. The testing of contingency plans is essential to determine whether the plans will function as intended. Without testing, agencies can have only minimal assurance that they will be able to recover mission-critical systems and processes in the event of an interruption.

Opportunities exist to improve the annual FISMA reporting process. For example, in the absence of an independent verification of agency-reported data, having a senior agency official attest to the accuracy of data could provide additional assurance.

In addition, performance measurement data do not indicate the relevant importance or risk of the systems for which FISMA requirements have been met. Reporting performance data by system risk would provide better information about whether agencies are prioritizing their information security efforts according to risk.

Finally, developing and adopting a commonly accepted framework for conducting the annual IG reviews mandated by FISMA could help to ensure consistency and usefulness of these reviews.

Mr. Chairman, this concludes my opening statement. I will be happy to answer any questions you or the members of the committee may have.

[The prepared statement of Mr. Wilshusen follows:]

United States Government Accountability Office

GAO

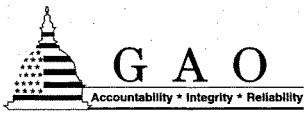
Testimony
Before the House Committee on
Government Reform

For release on delivery
expected at 10:00 a.m. EDT
Thursday, April 7, 2005

INFORMATION SECURITY

Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements

Statement of Gregory C. Wilshusen
Director, Information Security Issues



GAO-05-483T

Abbreviations

CIO	chief information officer
FISMA	Federal Information Security Management Act of 2002
IG	inspector general
IT	information technology
OMB	Office of Management and Budget
PCIE	President's Council on Integrity and Efficiency
NIST	National Institute of Standards and Technology

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-483T, a testimony before the House Committee on Government Reform

Why GAO Did This Study

For many years, GAO has reported that poor information security is a widespread problem that has potentially devastating consequences. Further, since 1997, GAO has identified information security as a governmentwide high-risk issue in reports to Congress—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 Inspectors General (IGs).
- Opportunities for improving the usefulness of the annual reporting process, including the consideration of a common framework for the annual FISMA reviews conducted by the IGs.

www.gao.gov/cgi-bin/getrpt?GAO-05-483T

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-3317 or wilshuseng@gao.gov.

April 2005

INFORMATION SECURITY

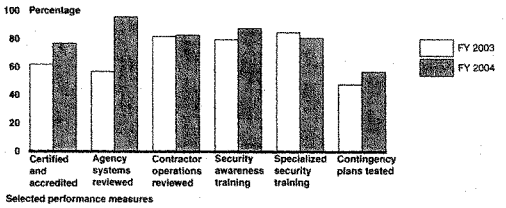
Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements

What GAO Found

In its fiscal year 2004 report to the Congress, OMB reports significant strides in addressing long-standing problems, 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). Fiscal year 2004 data reported by 24 major agencies generally show increasing numbers of systems meeting key statutory information security requirements compared with fiscal year 2003 (see figure). Nevertheless, challenges remain. For example, only 7 agencies reported that they had tested contingency plans for 90 to 100 percent of their systems, and 6 of the remaining 17 agencies reported that they had tested plans for less than 50 percent of their systems.

Opportunities exist to improve the usefulness of the annual FISMA reporting process, including enhancing the reliability and quality of reported information, providing performance information based on the relative importance or risk of the systems, and reporting on key information security requirements. In addition, a commonly accepted framework for the annual FISMA mandated reviews conducted by the IGs could help ensure the consistency and usefulness of their evaluations.

Percentage of Selected Performance Measurement Data for 24 Federal Agencies



Source: OMB's FY2003 and 2004 Report to Congress on Federal Government Information Security Management; GAO (analysis).

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss efforts by federal agencies and the administration 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] Further, since 1997, we have identified information security as a governmentwide high-risk issue in reports to the Congress—most recently in January 2005.[3] Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that made them vulnerable to attack, Congress passed FISMA, which permanently authorized and strengthened the federal information security program, evaluation, and reporting requirements established for federal agencies.

In my testimony today, I will summarize the reported status of the federal government's implementation of FISMA and the efforts by 24 major federal agencies[4] to implement federal information security requirements, including areas of progress and continuing challenges. I will also present opportunities for improving the usefulness of annual reporting on FISMA implementation.

[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).

[4] These 24 departments and agencies are the Departments of Agriculture, Commerce, Defense (DOD), Education, Energy, Health and Human Services, Homeland Security (DHS), 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.

In conducting this review, we reviewed and summarized OMB's fiscal year 2004 report to Congress on FISMA implementation.[5] We also reviewed and summarized the fiscal year 2004 FISMA reports for 24 of the largest federal agencies and their Inspectors General (IGs). In addition, we reviewed standards and guidance issued by OMB and the National Institute of Standards and Technology (NIST) pursuant to their FISMA responsibilities. We did not validate the accuracy of the data reported by the agencies or OMB, but did analyze the IGs' fiscal year 2004 FISMA reports to identify any issues related to the accuracy of agency-reported information. We performed our work from October 2004 to March 2005 in accordance with generally accepted government auditing standards.

Results in Brief

In its fiscal year 2004 report to the Congress, OMB noted that the federal government continued to make significant progress in identifying and addressing its security weaknesses, but that challenging weaknesses remain. In particular, the report identified several common deficiencies, such as the varying effectiveness of agencies' security remediation processes and the inconsistent quality of agencies' certification and accreditation processes.[6] The report also presented a plan of action that OMB is pursuing with agencies to improve performance.

In their fiscal year 2004 reports, the 24 major federal agencies generally reported an increasing number of systems meeting key statutory information security requirements, such as percentage of systems certified and accredited, number of systems and contractor operations reviewed annually, the percentage of employees and

[5]Office of Management and Budget, Federal Information Security Management Act (FISMA) 2004 Report to Congress, March 1, 2005.

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

contractors who received security training, and the percentage of systems with contingency plans tested. Nevertheless, challenges remain. For example, 17 agencies reported that they had tested contingency plans for less than 90 percent of their systems.

Opportunities exist to improve the usefulness of the annual FISMA reporting process, including enhancing the reliability and quality of reported information, completing and reporting accurate system inventories, providing performance information based on the relative importance or risk of the systems, reporting on key information security requirements, and clarifying reporting instructions in areas such as inventory and remediation plans. In addition, a commonly accepted framework for the annual FISMA reviews conducted by the IGs could help ensure consistency and usefulness of their evaluations.

Background

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

We recently reported that while federal agencies showed improvement in addressing information security, they also continued to have significant control weaknesses in federal computer systems that put federal operations and assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at the risk of disruption. The significance of these weaknesses led GAO to conclude in the audit of the federal government's fiscal year 2004

financial statements[7] that information security was a material weakness.[8] Our audits also identified instances of similar types of weaknesses in non-financial systems. Weaknesses continued to be reported in each of the six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation.

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

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

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

[8]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.

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. FISMA assigns specific responsibilities to agency heads, chief information officers, and IGs. It also assigns responsibilities to OMB, which include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security and reviewing at least annually, and approving or disapproving, agency information security programs.

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

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems;
- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;

- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

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

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

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

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

OMB Reporting Instructions and Guidance Emphasize Performance Measures

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

- certification and accreditation
- testing of security controls
- agency systems and contractor operations or facilities reviewed annually
- annual security awareness training for employees
- annual specialized training for employees with significant security responsibilities
- testing of contingency plans
- minimum security configuration requirements
- incident reporting

Further, OMB provided instructions for continued agency reporting on the status of remediation efforts through plans of action and

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

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

OMB Report to Congress Noted Progress and Challenges

In its March 1, 2005, report to Congress on fiscal year 2004 FISMA implementation,[9] OMB concluded that the federal government continued to make significant progress in identifying and addressing its security weaknesses but that much work remains. OMB assessed the agencies in their progress against three governmentwide security goals established in the President's 2004 budget:

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

- *Goal 1 — As required by FISMA, all federal agencies are to have created a central remediation process to ensure that program and system-level IT security weaknesses, once identified, are tracked and corrected. In addition, each agency IG is to verify whether the agency has a process in place that meets criteria specified in OMB guidance.* Based on IG responses to these criteria, OMB reported that each agency had an IT security remediation process, but that the maturity of these processes varied greatly. They did note that 18 agencies now have a remediation process verified by the IG, up from 12 in 2003.
- *Goal 2 — Eighty percent of federal IT systems are to be certified and accredited.* Although agencies have not reached this goal, they did come close, certifying and accrediting 77 percent of their systems.
- *Goal 3 — Eighty percent of the federal government's fiscal year 2004 major IT investments shall appropriately integrate security into the life cycle of the investment.* OMB reported that agencies have exceeded this goal by integrating security into the life cycle of 85 percent of their systems.

OMB also noted that, while progress has been made, deficiencies in security policy, procedure and practice continue to be identified at the agencies. Common deficiencies noted by OMB in its report were:

- *Agencywide plans of action and milestones.* Agencies had not fully implemented plans of action and milestones. The OMB report noted that IGs assessed the quality of their agencies' remediation process during 2004 and that six IGs identified overall deficiencies in their agencies' processes.
- *Quality of certification and accreditation process.* Agencies' certification and accreditation processes were inconsistent in quality. Fifteen IGs rated the agency process as good or satisfactory; however, seven IGs rated the process as poor and two did not report because they did not complete the evaluation.
- *Assessment of agency incident handling programs.* Agencies were not reporting security incidents consistently. OMB noted that agencies are required to notify and consult with the federal information security incident center operated by the Department of Homeland Security. However, the department's statistics indicate

sporadic security incident reporting by some agencies and unusually low levels of reported malicious activity at other agencies.

The report also outlined a plan of action to improve performance, assist agencies in their information technology security activities, and promote compliance with statutory and policy requirements. OMB has set a goal for agencies, that by June 2005 they will have all systems certified and accredited, have systems installed and maintained in accordance with security configurations, and have consolidated all agency infrastructure to include providing for continuity of operations.

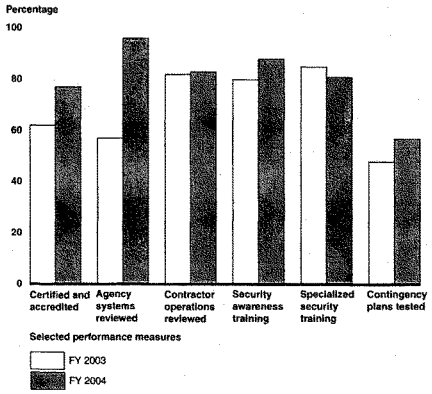
Agency FISMA Reports Highlight Increases in Performance Measures, but Challenges Remain

In their FISMA-mandated reports for fiscal year 2004, the 24 major agencies generally reported increases in their compliance with information security requirements as compared with 2003. However, analysis of key measures revealed areas where agencies face challenges. The following key measures showed increased performance and/or continuing challenges:

- percentage of systems certified and accredited;
- percentage of agency systems reviewed annually;
- percentage of contractor operations reviewed annually;
- percentage of employees 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 the reported overall status of the 24 agencies in meeting these performance measures and the increases between fiscal years 2003 and 2004. Summaries of the results reported for the specific measures follow.

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



Source: OMB's FY2003 and 2004 Report to Congress on Federal Government Information Security Management; GAO (analysis).

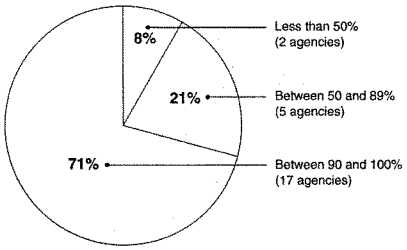
Certification and Accreditation

Included in OMB's policy for federal information security is a requirement that agency management officials formally authorize their information systems to process information and, thereby, accept the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan. 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 overall increases for most agencies. For example, 19 agencies reported an increase in the percentage of their systems that had completed certification and

accreditation. Overall, 77 percent of the agencies' systems governmentwide were reported as certified and accredited, compared to 62 percent in 2003. In addition, 17 agencies reported 90 percent or more of their systems had successfully completed the process, as illustrated in figure 2.

Figure 2: Percentage of Systems during Fiscal Year 2004 that are Authorized for Processing after Certification and Accreditation



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

However, as we previously reported, our analysis of the certification and accreditation of 32 selected systems at four agencies[10] identified instances where appropriate criteria were not always met. For example, we noted instances in which systems were accredited even though risk assessments were outdated, contingency plans were incomplete or untested, and control testing was not performed. Further, in some cases, documentation did not clearly indicate what residual risk the accrediting official was actually accepting in making the authorization decision. As such, agency reported performance data may not accurately reflect the status of an agency's efforts to implement this requirement.

[10]GAO, *Information Security: Agencies Need to Implement Consistent Processes in Authorizing Systems for Operations*, GAO-04-376, (Washington, D.C.: June 28, 2004).

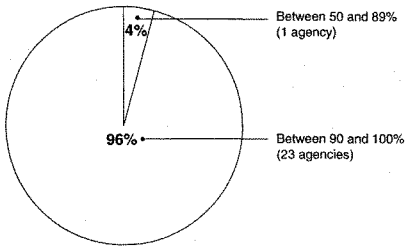
The information reported for certification and accreditation has taken on new importance this year as OMB has changed the reporting requirements for 2004. In 2003, agencies were required to report separately on risk assessments and security plans. In 2004, OMB eliminated this separate reporting in its guidance and directed agencies to complete risk assessments and security plans for the certification and accreditation process to be accomplished. As a result, the performance measure for certification and accreditation now also reflects the level of agency compliance for risk assessments and security plans.

Annual Review of Agency Systems

FISMA requires that agency information security programs include periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices to be performed with a frequency that depends on risk, but no less than annually. This is to include testing of management, operational, and technical controls 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. Further, management control testing and evaluation as part of program reviews is an additional source of information that can be considered along with control testing and evaluation in IG and GAO audits to help provide a more complete picture of the agencies' security postures. As a performance measure for this requirement, OMB requires that agencies report the number of systems that they have reviewed during the year.

Agencies reported a significant increase in the percentage of their systems that underwent an annual review. Twenty-three agencies reported in 2004 that they had reviewed 90 percent or more of their systems, as compared to only 11 agencies in 2003 that were able to report those numbers (see figure 3).

Figure 3: Percentage of Systems Reviewed During Fiscal Year 2004



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

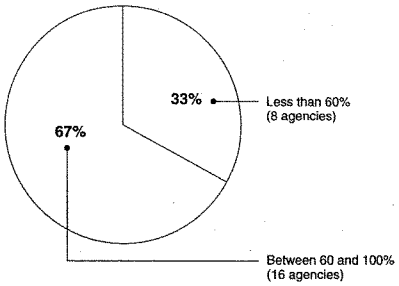
Annual security testing helps to provide assurance to the agencies that security controls are in place and functioning correctly. Without such testing, agencies cannot be assured that their information and systems are protected.

Annual Review of Contractor Operations

Under FISMA, agency heads are responsible for providing information security protections for information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor. Thus, as OMB emphasized in its fiscal year 2003 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. This underscores longstanding OMB policy concerning sharing government information and interconnecting systems: federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls.

The key performance measure of annually reviewing contractor operations showed a minor increase from 80 percent in 2003 to 83 percent in 2004. Although there was an increase overall, 8 agencies reported reviewing less than 60 percent of their contractor systems, twice the number of agencies reporting that level in 2003. The breakdown of the percentages of contractor operations reviewed by agency is provided in figure 4.

Figure 4: Percentage of Contractor Operations Reviewed during Fiscal Year 2004



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

Security Awareness Training

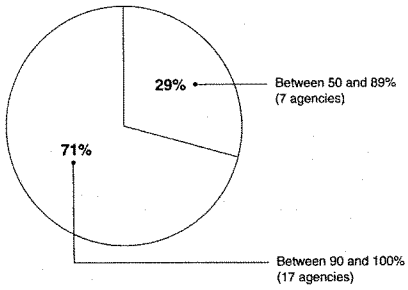
FISMA requires agencies to provide security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities, and the agency's responsibilities in complying with policies and procedures designed to reduce these risks. Our studies of best practices at leading organizations[11] have shown that such

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

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

The majority of agencies reported increases in the number of individuals who had received basic security awareness training. Seventeen agencies reported that they had trained more than 90 percent of their employees and contractors in basic security awareness (see figure 5).

Figure 5: Percentage of Employees and Contractors who Received IT Security Awareness Training in Fiscal Year 2004



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

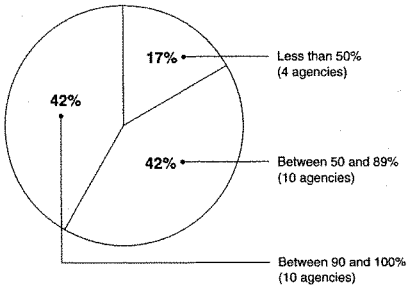
That figure represents an improvement over 2003, when only 13 agencies reported a 90 percent or higher rate.

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 have shown that such organizations recognized that staff expertise needed to be updated frequently to keep security employees updated on changes in threats, vulnerabilities, software, security techniques, and security monitoring tools. OMB directs agencies to report on the percentage of their employees with significant security responsibilities who received specialized training.

Agencies reported varying levels of compliance in providing specialized training to employees with significant security responsibilities. Ten agencies reported that they had provided specialized security training for 90 percent or more of these employees (see figure 6).

Figure 6: Percentage of Employees with Significant Security Responsibilities Who Received Specialized Security Training in Fiscal Year 2004



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

Note: Total does not add to 100 percent due to rounding

Moreover, 10 agencies reported a decrease in the number of such employees who received specialized training. Given the rapidly changing threats in information security, agencies need to keep their IT security employees up-to-date on changes in technology. Otherwise, agencies may face increased risk of security breaches.

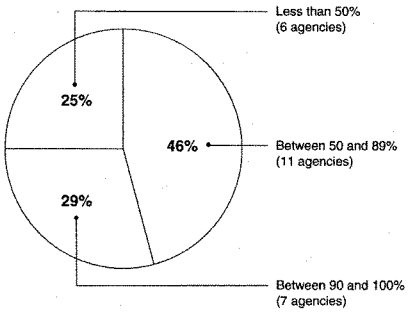
Testing of Contingency Plans

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

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

Agencies' reported fiscal year 2004 data for these measures showed that although 19 agencies reported increases, 6 agencies reported less than 50 percent of their systems had tested contingency plans (see figure 7).

Figure 7: Percentage of Systems with Contingency Plans that Have Been Tested for Fiscal Year 2004



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

Overall, federal agencies reported that 57 percent of their contingency plans had been tested. Without testing, agencies can have limited assurance that they will be able to recover mission-critical applications, business processes, and information in the event of an unexpected interruption.

Opportunities Exist to Increase Usefulness of Annual Reporting

Periodic reporting of performance measures for FISMA requirements and related analysis is providing valuable information on the status and progress of agency efforts to implement effective security management programs, thereby assisting agency management, OMB, and Congress in their management and oversight roles. Several opportunities exist to improve the usefulness of such information as indicators of both governmentwide and agency-specific performance in implementing information security requirements. In developing future reporting guidance, OMB can consider how their efforts can help to address

the following factors that affect the usefulness of the current annual reporting process.

- *Limited assurance of data reliability.* Currently, there is limited assurance of the accuracy of the data reported in the performance measures. The performance measures reported by the agencies are primarily based on self-assessments and are not independently verified. OMB did not require the IGs to verify agency responses to the performance measures. In addition, OMB does not require agency officials to attest to the accuracy of agency-reported performance data. In the absence of independent verification of data, such a statement could provide additional assurance of the data's accuracy.

- *Limited assurance of the quality of agency processes.* The performance measures offer limited assurance of the quality of the agency processes that generate the data. For example, the agencies report on the number of agency systems and contractor operations that they review annually. They also report on, and the IGs confirm, whether they used appropriate guidance. However, there is no reporting on the quality of the reviews, including whether guidance was applied correctly or if the results are tracked for remediation. OMB has recognized the need for assurance of quality for some agency processes. For example, it specifically requested the IGs to evaluate the plan of action and milestones process and the certification and accreditation process at their agencies. The results of these evaluations call into question the reliability and quality of the performance data reported by several agencies. As a result, increased risk exists that the performance data reported by the agencies may not be reliable or accurate.

- *Accuracy of agency system inventories.* Accurate inventory data would increase reliability of the reporting measures. While significantly more agencies reported having accurate inventories in the 2004 reports than in 2003, four agencies reported that they did not have accurate inventories. The total number of agency systems is a key element in OMB's performance measures, in that agency progress is indicated by the percentage of total systems that meet specific information security requirements. Thus, inaccurate or incomplete data on the total number of agency systems affects the

percentage of systems shown as meeting the requirements. Further, a complete inventory of major information systems is a key element of managing the agency's IT resources, including the security of those resources. Twenty agencies reported having inventories of their major systems in their 2004 reports, whereas in 2003 only 13 agencies responded affirmatively. However, 16 IGs reported that they did not agree with the accuracy of their agency's inventory. Without reliable information on agencies' inventories, the agencies, the administration, and Congress can not be fully assured of agencies' progress in implementing FISMA.

- *Data reported in aggregate, not according to agency risk.* Performance measurement data are reported on the total number of agency systems but do not indicate the relative importance or risk of the systems for which FISMA requirements have been met. The Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems,*[12] requires agencies to categorize their information systems according to three levels of potential impact on organizational operations, assets, or individuals should a breach of security occur—high (severe or catastrophic), moderate (serious), and low (limited). Reporting information by system risk would provide better information about whether agencies are prioritizing their information security efforts according to risk. For example, the performance measures for fiscal year 2004 show that 57 percent of the total number of systems have tested contingency plans, but do not indicate to what extent this 57 percent includes the agencies' most important systems. Therefore, agencies, the administration, and Congress cannot be sure that critical federal operations can be restored if an unexpected event disrupts service.

- *Reporting on key FISMA requirements.* FISMA requires agencies to have procedures for detecting, reporting, and responding to security incidents. Currently, the annual reporting developed by OMB focuses on incident reporting: how the agencies are reporting their

[12]National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems,* Federal Information Processing Standards Publication (FIPS PUB) 199, December 2003.

incidents internally to law enforcement and to the U.S. Computer Emergency Readiness Team at the Department of Homeland Security. Although incident reporting is an important aspect of incident handling, it is only one part of the process. Additional questions that cover incident detection and response activities would be useful to oversight bodies in determining the extent to which agencies have implemented security incident handling capabilities. The annual reporting process does not include separate reporting on key FISMA requirements. For example, in the 2004 guidance, OMB eliminated separate reporting on risk assessments and security plans. Because NIST guidance on the certification and accreditation process requires both risk assessments and security plans, OMB did not require agencies to answer separate questions on risk assessments and security plans. Although OMB asked for the IGs' assessment of the certification and accreditation process, it did not require them to comment on these specific requirements.

- *Clear reporting instructions.* Several questions in OMB's 2004 reporting guidance relating to agency inventories, plans of action and milestones, certification and accreditation process, and system configuration requirements could be subject to differing interpretations by IGs and the agencies. For example, one of the questions asked the IGs whether they and their agency used the plan of actions and milestones as a definitive management tool. However, IGs are not required to use these plans. Therefore, a negative answer to this question could mean either that the agency and the IG was not using the plan, or that one of them was not using the plan. Discussions with agency officials and IGs and our analysis of their annual reports indicate that they interpreted several questions differently. Another example was one of the inventory questions. It asked if the IG and agency agreed on the number of programs, systems, and contractor operations in the inventory. Since the question could be interpreted two ways, the meaning of the response was unclear. For example, if an IG replied in the negative, it could mean that, while the IG agreed with the total numbers in the inventory, it disagreed with the agency's categorization. Alternatively, a negative response could mean that the IG disagreed with the overall accuracy of the inventory. Clarifying reporting instructions could increase the reliability and consistency of reported performance data.

- *Accepted framework for IG reviews.* A commonly accepted framework for the annual reviews conducted by the IGs under FISMA could help ensure the consistency and usefulness of their evaluations. Because a commonly accepted framework currently does not exist for the IGs, they do not have a common methodology. This inconsistency can affect the consistency and comparability of reported results, potentially reducing the usefulness of the IG reviews for assessing the governmentwide information security posture. The IG community has recognized the importance of this issue. Working through the President's Council on Integrity and Efficiency, the IGs are working to develop a framework for FISMA reviews. They are including both OMB and GAO in their deliberations. The President's Council on Integrity and Efficiency is composed of IGs who are appointed by the President. The Council currently maintains *The Financial Audit Manual* in cooperation with GAO, which brings expertise and experience to the development of a FISMA review framework.

In summary, through the continued emphasis of information security by the Congress, the administration, agency management, and the audit community, the federal government has seen improvements in its information security. However, despite the progress shown by increases in key performance measures, challenges still exist. Accordingly, if information security is to continue to improve, agency management must remain committed to these efforts. The annual reports and performance measures will continue to be key tools for holding agencies accountable and providing a barometer of the overall status of federal information security. It is therefore essential that agencies' monitoring, review, and evaluation processes provide Congress, the administration, and IG and agency management with assurance that these measures accurately reflect agency progress.

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) 512-3317 or Suzanne Lightman, Assistant Director, at

(202) 512-8146. We can also be reached by e-mail at wilshuseng@gao.gov and lightmans@gao.gov, respectively.

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

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

PRINTED ON RECYCLED PAPER

Chairman TOM DAVIS. Thank you. We do have a number of questions.

Ms. Evans, thanks for being with us.

STATEMENT OF KAREN S. EVANS

Ms. EVANS. 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.

In March 2005 OMB issued our second annual report on implementing the Federal Information Security Management Act [FISMA]. We continue to believe FISMA provides a sound foundation for improving and maintaining a strong Federal information technology security program. In short, FISMA is working. Results are apparent. Agencies and Inspectors General are becoming more acclimated to its requirements, and new technical guidelines from the National Institute of Standards and Technology are coming online to promote further progress. We see no need at this time to revise it in any significant way, in fact, substantial revision could delay additional progress.

Across the Federal Government, most agencies have shown substantial progress in improving their information security programs. In addition, for the first time agencies reported the degree to which they've implemented security configurations for operating systems and software applications. We found that all agencies have begun developing and implementing security configuration policies for at least some of their operating systems.

While progress has been made, deficiencies in agency security procedures and practices remain. Two common deficiencies noted by the agency's Inspector Generals include weaknesses in agency-wide plans of actions and milestones, and the lack of quality in some of the agencies' certification and accreditation processes.

In addition, we have identified other areas of concern; they include overall inconsistency in agency and government-wide FISMA implementation, self and IG evaluations. Potentially unnecessary duplication of effort and resources across the government, ensuring adequate security of contractor-provided services, and a transition to Internet protocol version 6.

While we believe FISMA itself, along with the implementing guidance from OMB, NIST, and the national security authorities are sufficiently comprehensive and detailed to address these concerns at a policy level. Consistent implementation is difficult and requires considerable expertise and resources at the agency.

I would like to answer directly one of the questions asked in your invitation letter, whether there is a need for the Inspector General auditing framework similar to that used in financial audits. We have found the IG's analysis extremely valuable in gaining additional insight into the agency's IT security programs and operations. Much of the analysis in our annual report comes from the IG's findings, but at the same time, like agency CIOs and operational program officials, IGs have varying capacities in the areas of resource available and security expertise.

And across the IG community, there are differing methodologies and perspectives on what comprises a sound security program, in-

cluding the proper way to implement FISMA. Therefore, to the extent that an IG framework would promote greater consistency, we would support it; but we do note a few concerns; first and foremost, we strongly believe that the work of the IG should, to the maximum extent practical, be integrated with and not separate from agency IT security programs; and second, we're concerned with the adoption of a strict and specific review requirement for FISMA purposes if they would, in any way, limit the essential interaction needed between IGs and CIOs.

In addition to ongoing discussions to promote consistency in oversight and reporting, we have asked the IGs to participate in the newly formed IT security line of business. We expect this line of business will not only lead to a de facto IG and CIO reporting framework, but more importantly, a stronger Federal Government-wide IT security program.

While the task force performs its work, OMB will continue to use our existing oversight mechanisms to improve agency and government-wide IT security performance. Information technology security is one of the No. 1 critical components that agencies must implement in order to achieve green for the e-government initiative of the President's management agenda. If the security criteria are not successfully met, agencies cannot move forward regardless of their performance against the other criteria.

In conclusion, over the past year agencies have made significant progress in closing the Federal Government information technology security performance gaps.

I would like to acknowledge the significant work of the agencies and the IGs in conducting the annual reviews and evaluations. While notable progress in resolving IT security, weaknesses have been made, problems continue, and new threats and vulnerabilites continue to materialize. To address these challenges OMB will continue to work with the agencies, GAO and Congress to promote appropriate risk-based and cost-effective IT security programs, policies and procedures to adequately secure our operations and assets. But again, we believe FISMA is more than adequate in its current form to support all the needed improvement efforts. I would be glad to take any questions at this time.

[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

April 7, 2005

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.

Today I would like to discuss the progress we have made in improving the security of the government's information technology, highlight a few remaining challenges, and identify the steps we are taking to address those challenges. In doing so, I will also address your specific areas of interest.

In March, 2005, OMB issued our second annual report on implementing the Federal Information Security Management Act (FISMA). Much of the information I am discussing today is provided in more detail in our report.

Through our efforts over the past several years overseeing the implementation of FISMA (and its predecessor the Government Information Security Reform Act) we continue to believe FISMA is a sound foundation for improving and maintaining a strong Federal information technology security program – covering both the security of systems and promoting the protection of valuable information.

In short FISMA is working, results are apparent, agencies and Inspectors General are becoming more acclimated to its requirements, and new technical guidelines from the National Institute of Standards and Technology are coming on line to promote further progress. We see no need at this time to revise it in any significant way. In fact, substantial revision could delay additional progress.

Progress in Improving Agency Security Programs

Across the Federal government, through their efforts to implement the requirements of FISMA, most agencies have shown substantial progress in improving their information security programs. Most notably, progress can be shown in increased certification and accreditation of systems, greater annual testing of security controls, more testing of contingency plans, early use of secure system configurations, and improved identification and tracking of security weaknesses.

In our March report to Congress we outlined the progress in the below areas because we believe they are good indicators of the overall health of agencies' security programs. Specifically we reported:

- Certification and accreditation of systems increased to 77% from last year's 62%. In terms of numbers of systems this is an improvement from 4,969 to 6,607 out of a total of over 8,000. Our report highlights the outstanding progress of the Department of Labor (moving from 58% to 96%) and the Department of Transportation (from 33% to 98%).

- Annual testing of system controls increased to 76% percent from last year's 64%. In terms of numbers of systems this is an improvement from 5,143 to 6,515 out of a total of over 8,000.

- Contingency planning increased to 75% from last year's 68% and testing of these plans showed an increase to 57% from last years 48%. The latter is an increase from 3,835 systems to 4,886 out of a total of more than 8,000.

- Finally, in FY 2004, for the first time, agencies reported the degree to which they implemented security configurations for operating systems and software applications. All agencies have begun developing and implementing security configuration policies for at least some of their operating systems.

Securing Agency Critical Infrastructures and Developing Standard Identifications for Federal Employees and Contractors

Related to the goals of FISMA, we are also working with the agencies to improve the identification, prioritization, and security of their critical IT infrastructure. Under the requirements of Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," agencies submitted to OMB plans to protect their critical infrastructure. Working together, OMB and the Department of Homeland Security have evaluated and provided further instructions to the agencies for improvements and next steps.

Additionally, at the President's direction in Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," we have aggressively developed and will soon begin implementing a uniform identification standard for both physical access to Federal facilities and logical access to Federal IT systems.

Our objective is to ensure the identification for government employees and contractors is reliable and can be easily and quickly verified (both visually by a security guard at the front desk and electronically). We know agencies are investing millions of dollars annually in incompatible identification processes and systems, some with questionable value and performance. We also recognize some identifications currently issued by Federal agencies could be forged or stolen thus compromising the

government's employees and contractors as well as physical, information, and information technology assets.

Following considerable public notice and comment, including several public meetings, in February 2005 the National Institute of Standards and Technology (NIST) issued the Federal Information Processing Standard (FIPS) 201: "Personal Identity Verification for Federal Employees and Contractors". Agencies will begin implementing the standard in October of this year.

Continuing Challenges

While progress has been made, deficiencies in agency security procedures and practice remain, much of it due to inconsistent implementation within agencies and across the government. Continuing weaknesses reflect the complexity of securing the Federal government's vast number of information systems. Examples of common deficiencies noted by agency Inspectors General (IGs) include:

- Agency-wide Plans of Action and Milestones (POA&Ms). OMB asked agency IGs to assess, against specific criteria, the quality of the agency-wide POA&M process. OMB policy requires agencies to prepare POA&Ms for all programs and systems where an IT security weakness has been found. Although 18 IGs have verified their agency's management of an effective POA&M process, six IGs revealed overall deficiencies in their agency's process.

- Quality of certification and accreditation process. This year for the first time, IGs were asked to assess the overall quality of their agency's certification and accreditation process, including the degree to which agencies follow NIST guidance. Six IGs rated the agency certification and accreditation process as "good", and nine rated it as "satisfactory;" however, seven IGs rated the process as "poor" and two were not able to complete the evaluation. None of the IGs rated the certification and accreditation process as failing.

In addition to deficiencies noted by the agency IGs, we have identified other areas of concern through our own reviews and in consultation with other experts including the agencies and the Government Accountability Office (GAO). Some of these areas are new while others continue from prior years. They include:

- Overall inconsistency in agency and government-wide FISMA implementation and self-evaluations and IG evaluations
- Potentially unnecessary duplication of effort and resources across government
- Ensuring adequate security of contractor provided services
- Transition to Internet Protocol Version 6

While we believe FISMA itself and implementing guidance from OMB, NIST, and national security authorities is sufficiently comprehensive and detailed to address these concerns at a policy level, consistent implementation is difficult and requires

considerable expertise and resources from each agency (including small and independent agencies).

Below, I will address some specific plans to address the above challenges, but first I want to begin by answering directly one of the questions asked in your invitation letter, i.e., whether there is a need for an IG auditing framework similar to that used in financial audits?

We have found the IG's analysis extremely valuable in gaining additional insight into agency IT security programs and operations. Much of the analysis in our annual report, and we know your annual security report card, comes from the IG's findings. We have been able to use this information to validate agency reports and better hold agencies accountable in various ways including through the President's Management Agenda Scorecard process.

At the same time, like the agencies themselves (including CIOs and operational program officials), across the IG community IGs have varying capacities including available resources to conduct comprehensive reviews, different levels of security expertise, and across the IG community differing methodologies and perspectives on what comprises a sound security program and what constitutes proper implementation of FISMA and OMB policies. As a result, we have found relying solely on an IG's assessment is not always adequate.

Therefore, to the extent an IG evaluation framework would promote greater consistency we would support it. However, we do note the concerns below.

First and foremost, we strongly believe the work of the IGs should to the maximum extent practicable, be integrated into and not separated from agency IT security programs. This is especially important to avoid agencies' and IGs competing for scarce security expertise—taking away essential resources needed to implement and maintain security programs and shifting them to IG specific evaluations. We have already seen examples of this shift in several agencies and are troubled by it. It does not in our view promote sound security programs. We have stressed the importance of interaction in our FISMA implementing guidance. Again, the IGs and the agencies should work together throughout the year, share resources to the maximum extent practicable, and improve the overall program, not simply produce better evaluation reports. Furthermore, IGs and agencies should also share findings from program and system reviews as they become available. OMB encourages IGs to deliver interim reports to agency officials in instances where potential significant deficiencies have been identified. Timely sharing and awareness of security weaknesses and significant deficiencies helps prevent further loss and damage to the agency's overall performance.

Second, we are concerned with adopting strict and specific review requirements for FISMA purposes if they would in any way limit the essential interaction described above. We are particularly concerned with requiring IGs to perform an "audit" as opposed to FISMA's "evaluation." By requiring an evaluation but not an audit, FISMA

intended to provide IGs flexibility as to the degree of cooperation with CIOs and program officials. OMB encourages IGs to take advantage of this flexibility while ensuring the appropriate degree of accuracy, independence, and objectivity. Moreover, unless any review requirements were very closely aligned with OMB's implementing policies and NIST guidance, agencies could be evaluated by IGs against one set of criteria and by OMB against another different set. We see this today when IT security programs are evaluated by IGs using the Federal Information Systems Control Audit Manual (FISCAM). While FISCAM's underlying principles are essentially the same as OMB's security policies, there are sufficient differences in the specific details as to make easy correlation unnecessarily complex, time-consuming and in some cases unhelpful.

Throughout the past several years, we have had ongoing discussions with key members of the IG groups to solicit feedback on the FISMA reporting and evaluation process. In particular this year, we have engaged the President's Council on Integrity and Efficiency and we have discussed ways to make their evaluations more consistent.

Also to promote increased consistency in oversight and reporting, we have asked the IGs to participate in OMB's newly formed IT Security Line of Business which I discuss in greater detail below. We expect this line of business will not only lead to a *de facto* IG and CIO reporting framework, but, more importantly a stronger Federal government-wide IT security program.

Activities to Improve IT Security Performance

IT Security Line of Business

On March 23, 2005, OMB kicked off an information systems security line of business co-managed by the Department of Homeland Security and the National Security Agency. Since the kick-off, an interagency task force has formed and met twice. The task force comprises representatives from all 24 CFO Act agencies, the Small Agency Council, the IG community, and NIST.

In just two weeks the task force has come to consensus on its vision and goals. On Monday, April 4 it released a public request for information soliciting IT security best practices from industry and government.

The vision of the line of business task force is:

> *"The Federal Government's information systems security program enables agencies' mission objectives through a comprehensive and consistently implemented set of risk-based, cost-effective controls and measures that adequately protects information contained in Federal Government information systems."*

To achieve the vision, the task force has set the following goals:

- Identify problems and propose solutions to strengthen the ability of all agencies to identify and manage information security risks,
- Develop improved, consistent, and measurable information security processes and controls across government, and,
- Achieve savings or cost-avoidance through reduced duplication and economies of scale.

In order to achieve the vision and work towards the goals, the task force has identified five activity areas for consideration in the development of common IT security solutions. These five areas closely map to FISMA and include: training; threat awareness and incident response; program management; security in the systems lifecycle development process; and selection, evaluation, and implementation of security products.

Over the next few months, task force members will be gathering and analyzing information in these areas to develop recommendations for each of the five areas which could most benefit from a common solution, collaboration, or standardization of processes. Consolidated business cases will then be developed to implement any common solutions and inform the agencies' FY 2007 budget requests and OMB's decisions.

President's Management Agenda Scorecard

While the task force performs its work, OMB will continue to use our existing oversight mechanisms to improve agency and government-wide IT security performance. Specifically, as I have described to the Committee in the past, we are using the President's Management Agenda Scorecard and quarterly reporting process to drive agency progress.

By including IT security in the PMA Scorecard, we underscore while it clearly has a technical component, it is at its core an essential management function. Therefore, we have greatly increased executive-level attention and accountability.

As you know, the PMA was launched in August 2001 as a strategy for improving the performance of the Federal government. The PMA includes five government-wide initiatives, including Expanded Electronic Government (E-Government). The goals of the E-Government initiative are to ensure the Federal government's annual investment in information technology significantly improves the government's ability to serve citizens and to ensure systems are secure, delivered on time and on budget.

Each quarter, agencies provide updates to OMB on their efforts to meet government-wide goals. The updates are used to rate agency progress and status as either red (agency has any one of a number of serious flaws), yellow (agency has achieved intermediate levels of performance in all the criteria), or green (agency meets all the standards for success).

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 move forward, regardless of their performance against other E-Government criteria. 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:

- Demonstrate consistent progress in remediation of security weaknesses
- Attain certification and accreditation of ninety percent of their operational systems, and,
- Maintain an IG assessed and verified agency POA&M process.

In order to "maintain green," by July 1, 2005, agencies must have:

- Certified and accredited all systems,
- Installed and maintained all systems in accordance with security configurations, and,
- Consolidated and/or optimized all agency infrastructure to include providing for continuity of operations.

Integrating IT Security into the Budget Process

OMB policy requires agencies to submit a Capital Asset Plan and Business Case justification for all major information technology investments. In their justification, 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 assessed against specific criteria including whether the system's security, planned or in place, is appropriate.

Transition to Internet Protocol Version 6 (IPv6)

Late last fall, OMB directed the agencies to provide a preliminary report on their planning activities for the transition to IPv6 from the current IPv4. Only the Department of Defense has undertaken any significant activity in this area.

Since that time, the Department of Commerce and the Government Accountability Office have produced draft reports on the complexity and risks associated with this transition. While I am not prepared to nor should I discuss the details of these draft reports, I can say OMB is sufficiently concerned the complexities of the transition require special action. Therefore, we will begin, through the CIO Council, developing a comprehensive transition planning guide. We have yet to finalize the details for this activity, but will begin this effort soon.

Conclusion

Over the past year, agencies made significant progress in closing the Federal government's information technology security performance gaps. I would like to acknowledge the significant work of agencies and IGs in conducting the annual reviews and evaluations. This effort gives OMB and Congress much greater insight into agency IT security status and progress.

However, uneven implementation of security measures across the Federal government leaves vulnerabilities to be corrected. I have described the ways OMB will use existing management and budget processes and the new line of business to promote greater compliance with law, policy, and guidance and thereby improve agency-specific and the government-wide security program.

While notable progress in resolving IT security weaknesses has been made, problems continue and new threats and vulnerabilities continue to materialize. Much work remains to improve the security of the information and systems that support the Federal government's missions. To address these challenges, OMB will continue to work with agencies, GAO, and Congress to promote appropriate risk-based and cost-effective IT security programs, policies, and procedures to adequately secure our operations and assets.

But again, we believe FISMA is more than adequate in its current form to support all needed improvement efforts.

Chairman TOM DAVIS. Well, thank you both.

Ms. Evans, what changes or improvements is your office proposing for the 2005 FISMA guidance? And do you plan to issue new updated guidance regarding your circular A–130?

Ms. EVANS. We are working right now with the IG community and NIST, CNSS and GAO to revise the reporting requirements. It's going to be similar to last year. We are going to focus this year more on performance metrics, and we are we going to include a new reporting requirement this year dealing with privacy of the information that the agencies are collecting.

Chairman TOM DAVIS. Well, some agencies have expressed concern that the term "system" is not well defined; for instance, how should an agency classify a state system that contains Federal data? Does OMB plan to address this in the new guidance?

Ms. EVANS. The definition of a system—and I want to answer this question both from my past experience as an agency CIO, and now as the policy official.

The reason why I believe that we have allowed the definition to be the way that it is is that it provides maximum flexibility. So as agencies would potentially view this as ambiguous, we view it from a policy perspective as giving the agencies flexibility that they need to be able to determine and analyze what risk is appropriate for assets within their control that they have that they are responsible for.

So there is an ambiguous nature to the definition of system, but we look at it as it allows the flexibility for the agency to define that so that they can then go forward and implement the management policies and procedures they need in order to deal with that.

You could do something very small and say one piece—there could be an application on one piece that has enormous risk that it would impose if it was connected to a network; you may determine that should be called a system, and go through the full certification and accreditation for that. And a system could be as huge as a network, where the whole department's network, that can constitute a system because there are certain rules of engagement that you would want to have, rules of behavior on that system before you would go forward and allow other resources to be connected to it. So we don't necessarily want to go down and be so proscriptive in our definitions as to restrict the ability of the agency to be able to go forward and determine what is the best posture for them.

Chairman TOM DAVIS. But you could have agencies defining it differently, basically.

Ms. EVANS. They may, and that is why the evaluation that is being done by the IG, the independent evaluation coming in, looks at how they apply that definition, how they have a methodology within their department to see if the thought process that they put behind it to determine it is sound to address the risk.

Chairman TOM DAVIS. OK. Mr. Wilshusen, what do agencies have to do to get information security removed from the GAO high-risk list? This is, as you know, the list was expanded to include cyber security—well, cyber critical infrastructure protection. Information security has been on the list since 1997. Can you briefly discuss what you think needs to be done to get this off the high-risk list?

Mr. WILSHUSEN. Well, first of all, what they need to do—and where we have consistently found on our review—is to implement at each agency an effective agency-wide information security program, such as those principles and requirements embodied in FISMA. And we have found that many of the agencies have not done that. This in turn has allowed and has resulted in many of their systems being insecure.

Chairman TOM DAVIS. Now why don't they do that? Is it lack of money, they've got so many priorities at this point this is just one, without additional resources, that they're reluctant to do?

Mr. WILSHUSEN. It is probably a couple of issues. Certainly the emphasis and level of attention since the passage of FISMA has helped and has improved both awareness and accountability of the highest levels of each of the agencies, and that has been a positive thing. But in many cases it's primarily management issues, even though security has technical aspects to it. Many of the findings and issues that we identify are the result of management issues where certain requirements are just not being implemented.

Chairman TOM DAVIS. OK. Thank you very much. I'm going to have some more questions, but Mr. Ruppersberger is going to get a turn here.

Mr. RUPPERSBERGER. Well, after looking at the reports and the grades, I see that some agencies have improved. Is there any effort to have a departmental roundtable to share best practices? I mean, what we are really here for today is to try to get us to a level where we are going to be a lot more efficient, and we have to find a way to do this. And it seems to me, when you have agencies that are doing well and agencies that aren't doing well, let's look at it and share information.

Could either one of you address that issue?

Ms. EVANS. Yes, sir, I would be glad to.

There is actually two efforts underway. One the chairman already noted, which is the cyber security line of business. This is an interagency government-wide task force that OMB has brought together under the leadership of the Department of Homeland Security as well as it is being co-chaired by NSA. And what we are doing there is looking at all of the issues. There are four particular areas that we are looking at, like training, like management practices of framework, those types of activities which get to the heart of your question, what is working, and what can we take that is working within the agencies and move it out government-wide?

The one thing that when we set up this task force is, because of the way FISMA is set up and the way that a cyber security program should work, a good IT program should work within a department is you still have to look at the risk. Each department may have a different level of risk, so you can't necessarily think that one size would fit all. But that is what the security line of business is looking at.

Also, on the CIO council, the Department of Justice Vance Hitch, is our cyber security liaison; he works very closely with our Best Practices Committee on topics, and topics such as security have always been on the forefront to bring together the appropriate groups so that we can share best practices. And then also, there is a newly named forum that we are—the CIO council is co-chairing with Con-

gressman Davis' staff, which is the Chief Information Security Officers Forum.

So we are trying to bring it together at multiple levels within an organization, and across the government as a whole, so that practices can be identified——

Mr. RUPPERSBERGER. Let me ask you this question: So much of whatever we do in management, managing large organizations, whatever, is accountability, and also giving the resources to the people that we want to perform the mission. How about the issue of maybe a government-wide audit standard? Do you think that would help in this situation? It seems that we need a standard for all of our agencies. Now we have different missions and different areas that we move into. What do you think of that issue?

Ms. EVANS. Well, I believe, through the President's management agenda, that we have added specific criteria into the score card under e-government, so we are holding the agencies accountable for their performance.

Mr. RUPPERSBERGER. But these failing grades are just not acceptable.

Ms. EVANS. I believe that the progress and the way that we are measuring progress—we have the same goals in mind, both the committee as well as the administration. How we are measuring progress may be a little bit different based on what the rating factors are based on what the committee has. You are specifically asking me about an auditing standard, and FISMA specifically makes a difference between audit and evaluation. And we really think that it's more of an evaluation because this really needs to be a collaborative effort within the entire department, because as you are talking about it, it is a management issue as well. If it turns into an audit situation, our concern is is that there won't be as much exchange, that it is more an evaluation——

Mr. RUPPERSBERGER. That's a good point. I'm near the end of my 5 minutes, I want to keep moving down another area.

I am very concerned about the issue of the failing grade with Homeland Security, and I guess it is your turn, Mr. Wilshusen. Why do you feel at this point that Department of Homeland Security has a failing grade? What can we do to move that to another level to get them a lot more proficient in this subject matter today?

Mr. WILSHUSEN. Well, first of all, Homeland Security does—and I guess you will talk to the CIO and IG on the next panel as well, but they have had a number of challenges that they need to overcome just in the creation of the department to——

Mr. RUPPERSBERGER. No question.

Mr. WILSHUSEN. And that has been pretty much a key factor in some of the challenges that they face. However, at the same time, only just recently have they established key positions within that department in terms of having a chief information security officer, and they have identified key individuals to be responsible for information security. But it will take quite a bit of an effort for them to kind of meld different systems to make sure there is appropriate accountability, and the alignment of the information security program at the department level with different operating entities. Right now there is apparently quite a bit of autonomy between the two.

Mr. RUPPERSBERGER. And we can develop that in the next panel also, I see my time is up.

Chairman TOM DAVIS. Ms. Norton.

Ms. NORTON. Thank you, Mr. Chairman.

I'm sorry I was detained and I did not hear the entire testimony, but what concerns me is the unevenness among the agencies. Mr. Ruppersberger asked about homeland security and there may be some reason why they haven't gotten most of their act together, but some of these agencies you would expect to do better, you would expect the Department of State to do better, you would expect the Nuclear Regulatory Agency not to go down.

And I note that the agencies look like they are in charge of this entire process. They are required to take the steps to do the inventory of their systems. And apparently in the survey, 70 percent of them said they wanted greater guidance in meeting the requirements. The report cards signify nothing, if not the need for greater guidance. I'm wondering if too much of this is left to agencies who have no expertise here either in choosing consultants in security aspects of computer systems; in fact, no agency really does have that expertise. I'm wondering if simply saying to the agencies, do this, has been sufficient, particularly when they themselves say they want greater guidance in meeting the requirements. And I suppose the obvious question is, do you agree, and where would such guidance come from? Are any steps being taken to offer greater guidance, given the rather pathetic reports that are indicated in the Federal computer security report card?

Ms. EVANS. First off, what we are trying to do from an administration perspective is avoid being very, very proscriptive in the policy because what we want to avoid is people just going down and cranking through—mechanically cranking through and getting checkmarks because you really want the practice to be engrained, and we were talking about management practices.

So in order to meet what we are hearing from the agencies about additional guidance, we did take that to heart, and that is why the cyber security line of business was announced. They are looking at very specific areas, and we are bringing in the expertise in order to complement the team that has been put together government-wide. There will be recommendations that come out of that task force, specifically about how to identify problems, how to move forward, how to make sure that we have consistent and measurable types of statistics, how to do good certification and accreditation, and how to achieve the things that they are being measured upon, because I do agree with you, you just can't say, here are the requirements, go out and do it, and not provide the help and assistance that they need, especially when they are asking for it.

So the products that will come out of the cyber security line of business we are very hopeful will address the issue of giving further guidance, without issuing new policies.

Ms. NORTON. I don't understand what you mean about policy—being proscriptive as to policy. As I understand it, they want greater guidance in meeting the requirements and a clarification of FISMA's assessment guidelines. I don't see where there is policy proscription involved in that.

Mr. WILSHUSEN. One of the sources that the agencies can look to is NIST. Since FISMA was enacted, it placed specifically a responsibility to NIST in preparing and providing guidance and requirements to agencies and implementing the various aspects of FISMA. Over the last several—2 years, NIST has come out with guidance, and indeed they are going to be coming out with some additional guidance in different areas going forward.

Ms. NORTON. Well, they can look to that, and they could have looked to that all along, I take it.

Mr. WILSHUSEN. Over the last couple of years they have issued new guidance.

Ms. NORTON. Well, all I can say is if the agency—if this large percentage of the agencies that is, a super majority say we need greater guidance, it does seem to me that whatever is in place is insufficient, and that the responsibility of the administration centrally is to assure that they get that guidance so that these pathetic grades do not come before the committee again.

Thank you very much, Mr. Chairman.

Chairman TOM DAVIS. Thank you very much.

The gentleman from Tennessee.

Mr. DUNCAN. Well, thank you, Mr. Chairman.

I remember when we passed the one agriculture bill, farm bill a few years ago, 2 or 3 years ago, the Wall Street Journal had an editorial—and the bill was called the Farm Security Act—and it said any time we have the word "security" in a bill, we ought to give it 4 times the scrutiny because they were putting the word "security" in every bill, and we were going to great, great expense, and not getting a lot of bang for the buck, so to speak.

And then I have also read and heard that every computer system is obsolete the day it's taken out of the box now because the technology is moving so fast. So the concerns I have—and I know Governor Gilmore from Virginia, who chaired the President's Commission on Security and Terrorism, he said—in his cover letter to the President, he said we must resist the urge to try to achieve total and complete computer because he said it's not attainable, and if we aren't careful, we will drain our resources from other things that are achievable.

So I guess the two concerns I have is, No. 1, the cost of some of these things, because what I read repeatedly, I remember the FBI came up with a computer system that we spent hundreds of millions on, and then they said it was a disaster after we had paid for it. So what do we do on the cost of some of these things? Are we looking at those costs and what we are getting for our money so we don't just go ridiculously overboard? And second, are we settling for a Mercedes instead of constantly seeking to get Rolls Royces in regard to these systems?

You've always got these companies that want to sell you more and better and newer, and I'm just wondering are we using a little common sense in regard to some of these things?

Mr. WILSHUSEN. Well, certainly you are absolutely right, there is no way to provide absolute assurance that you are going to prevent any particular security infractions or violations and the like. You can never give 100 percent assurance that you are going to be able to thwart all security threats.

What you have to do, and what FISMA requires, is that you have a risk-based program and process in which you assess the risk to your systems, and then come up with cost-effective measures to protect against those particular risks. And certainly, that is one of the key underpinnings of any information security program is having it based on risk.

Mr. DUNCAN. All right.

Yes, ma'am.

Ms. EVANS. As far as your question about evaluating the cost based on the cyber security program, every agency is required, as they bring forth their IT investments, to ensure that the cyber security aspect, the risk associated with implementing that system, is addressed, and the costs are included in the cost of that business case coming forward.

So they have to look at how to secure the system against the benefits that they are going to achieve for implementing that system to ensure that there is an adequate return on investment as they go forward.

So the business case process does get to your other concern about ensuring that cost is being adequately addressed as they go forward.

Mr. DUNCAN. Well, I just don't want to see us go ridiculously overboard on the costs, or in any other direction, and have to buy new computer systems at hundreds of millions or even billions of dollars worth of cost just because somebody comes up with a little better system the next year than we had the year before. I mean, we just can't afford to keep doing that. And then have us read and hear at hearings and read in the paper that systems that some department or agency bought 1 year, as soon as it's taken—as soon as it's put on line, it's not what it was promised to be. So I just hope you will take those considerations—those concerns into consideration.

Thank you very much, Mr. Chairman.

Chairman TOM DAVIS. Thank you very much. Let me do a couple of followups.

The annual scorecard reflects that many of the larger agencies have—consistently are poor performers, it may be because of the complexity of their system. Has OMB identified a trend here?

Ms. EVANS. We have gone through and looked at the issues associated with the larger agencies. I think it does get back to some of the other high level issues that have been raised by the committee themselves, which is proper attention from management and ensuring that the priorities are established within the Department to be able to move forward. And a lot of it has to do with the leadership aspect of giving the proper attention to the program.

So the way that we are trying to address that, again, is back to the accountability issue, putting the proper tools in place, working with the agencies, but using the President's management agenda to hold the cabinet secretaries accountable for their performance in this area.

Chairman TOM DAVIS. And CIOs could be great, but if the cabinet secretaries aren't paying attention, or the managers, it makes it a lot tougher, doesn't it?

Ms. EVANS. Right. So we are trying to make sure—the administration is trying to make sure—and is making sure through the President's management agenda—that the cyber security aspect of anything that they do is brought to the level of the attention of the Deputy Secretary and the Secretary, who are responsible for the overall programs of their department.

Chairman TOM DAVIS. Let me just talk about the certification and accreditation, this C and A process, so to speak. I know that one of OMB's objectives in its plan of action is having all the systems C and A'd. But many IGs are reported on a very inconsistent quality of agencies C and A process. If the number of certified and accredited systems is increased, but there is a question about the quality of the processes, should we question the value of that information? And I will ask Mr. Wilshusen to also respond.

Ms. EVANS. Well, I was going to say the shorter answer is yes, you should question the quality of that based on the IG's finding; and that gets back to making sure that we provide better guidance where the agencies are asking for that, and working with the IG community and working with the CIOs as to having a good credible certification and accreditation program so that it does insert the discipline of always constantly looking at the risk.

Mr. WILSHUSEN. And I would agree, you certainly do need to question those statistics.

You know, just looking at what the agencies have reported in terms of 77 percent of all the systems have been certified and accredited, but one of the key aspects of that is to have a testing contingency plan that you need in order to be certified and accredited, and yet the agencies are also reporting that only 57 percent of their systems have testing contingency plans. So just that, in and of itself, shows that there is some question about the reliability of that data.

Chairman TOM DAVIS. We are going to hear Daniel Matthews, who is the DOT's CIO, suggest in his testimony eliminating timing differences between the IG and the agency reports in order to create a common point in time for measuring the status of an agency's IT security program. I can see the merit of that change; I would appreciate any comments either of you might have on that.

Mr. WILSHUSEN. OK. In terms of having an as-of date, what that would typically allow would allow the IGs to be able to perhaps verify the information that the agencies are reporting on their report cards in their performance measures, if that is the goal of having such an as-of date. Similar to like on the financial statement report where we have the end of the fiscal year, and then the IGs have another 45 days to make the report on it. But other than that, you know, I'm not sure what the benefit would be.

Chairman TOM DAVIS. All right.

Ms. EVANS. I was going to say, I concur with that. And we are just—we would proceed with caution on an as-of date because we want to make sure that interaction between the IGs and the CIOs for their programs are ongoing, even while they are still doing this annual reporting as well. So there is nothing wrong with getting an as-of date in order to have consistency for reporting, as long as the other goals are met.

Chairman TOM DAVIS. OK. Thank you very much.

Mr. Ruppersberger.

Mr. RUPPERSBERGER. I just have one question of you, Ms. Evans.

The Federal Information Security Management Act extends a requirement from the Paperwork Reduction Act that agencies develop detailed inventories of their systems, and this seems to be a requirement that agencies have a struggle with. One official from the Department of Energy recently remarked that unless that agency overhaul gets decentralized structure, poor assessment under FISMA were guaranteed for years to come.

Do you think that there are ways that FISMA's inventory requirement could be changed to address such concerns, without compromising security?

Ms. EVANS. That is an issue that we are attempting to address with the change in the scorecard criteria as well. Chairman Davis brought up the fact that we are saying all systems need be to certified and accredited. At the heart of that requirement is getting to how agencies are identifying their inventory.

What we intend, and the issue that we brought forward to the Interagency Task Force is to get a best practice or lessons learned from the agencies that are scoring really well on how they got a handle on their inventory process, and be able to apply that out to the agency.

If at the end of that task force effort that is not possible, then we will look at other alternatives and make recommendations or changes to address the inventory issue.

Mr. RUPPERSBERGER. OK. And for 2004, three agencies did not submit independent IG reports to OMB for their annual report. Can you explain why agencies are not complying with the IG independent evaluation, and if they're not, what recommendations will you have so that we make sure they do?

Mr. WILSHUSEN. Well, one I think was in the case where they—I think that was from the previous year, when DOD and VA did not submit their report.

Mr. RUPPERSBERGER. And that is not an issue now?

Mr. WILSHUSEN. Not as much this year, I don't think.

Mr. RUPPERSBERGER. Well, you say not as much though; if it's not, let's talk about——

Mr. WILSHUSEN. OK. I'm sorry, right. No, I don't think that was a major issue.

Mr. RUPPERSBERGER. For any of the agencies.

Mr. WILSHUSEN. That's correct.

Mr. RUPPERSBERGER. OK. That's good news then.

Chairman TOM DAVIS. Anyone else with questions? Anything you would like to add to clarify anything?

Ms. EVANS. Well, the only thing, sir, I would like to add is that we appreciate the focus of the committee on this issue because, as you know, it is a continuing priority for the administration in that we want to continue to make sure that cyber security is at the forefront of everything that we do. You have to have this going forward and manage the risk as we continue to take more and more information and move more and more—and deploy more and more in technology. So thank you for your oversight.

Chairman TOM DAVIS. And thanks for what you're doing. I'll just say, all you need is a bad adverse cyber event and everybody is

going to be all over this thing and asking the questions that we're asking now, why wasn't this done. And I'm not sure who the fall guy will be, but it ain't gonna be me.

And the difficulty in the private sector in many ways are ahead of us because they always are looking at the downside, they have to look at that. In government, many times the managers will take the risk that it won't happen on my watch, and they will go ahead with some of their other priorities; and yet we know we're talking so people out there—for their reasons are trying get in. So we appreciate your efforts on this, and the CIO's efforts. I think a lot of this depends on how close our CIOs are working with the agency heads at the end of the day.

The other thing is, I think ultimately these FISMA report cards are going to have to be tied to funding because sometimes that's the only thing people understand, you can preach, you can give them boxes to check, but if you tie it to funding, that really gets their attention, and that may have to be the next step if we continue to see the occurrences we do with some of these report cards.

We're going to hear from some very good CIOs in the next panel that have just very difficult jobs. These are difficult jobs in some of these agencies where you are putting a lot of their elements together, some of them that have been not working well for a long time, but we'll get to that.

Anything you want to add?

Mr. WILSHUSEN. Right. And I would just like to also express my appreciation for these oversight hearings because this certainly does help to hold the agencies accountable for implementing information security, and also with light comes heat, and heat usually brings action. And hopefully the increase of attention that this committee brings will help to improve that as well——

Chairman TOM DAVIS. And a lot of times we're just oversight; in this case we have jurisdiction as well. The FISMA came out of this committee. We do share oversight responsibilities with the Commerce Committee and with the Homeland Security Committee on which I serve. And that's good, I think we want everybody looking at this. I want to see more focus on this from more committees and more questions answered, that's what gets agency heads' attention.

But Ms. Evans, we appreciate your efforts on this. Sometimes you're the voice out there in the wilderness crying, but I know you have—your bosses are behind what you're doing and everything as well, and we want to make sure you have the tools to get the job done.

Thank you very much. We will take about a 2-minute recess and set up for the next panel.

[Recess.]

Chairman TOM DAVIS. We are now going to move to our second panel, and it is a distinguished panel indeed. We appreciate having everybody back. Mr. Wilshusen, who is here to stay on to answer questions but doesn't need to be sworn in again. We have Bruce Crandlemire, who is the Assistant Inspector General for Audit, U.S. Agency for International Development. John Streufert, the Acting Chief Information Officer of the U.S. Agency for International Development. Mr. Frank Deffer, who is the Assistant Inspector General for Information Technology, Department of Home-

land Security. Steve Cooper, no stranger to this committee, the Chief Information Officer, Department of Homeland Security. Ted Alves, the Assistant Inspector General for IT and Financial Management, Department of Transportation. Daniel Matthews, the Chief Information Officer, Department of Transportation.

It is our policy that we swear all the witnesses in, so if you could just rise and raise your right hands. Can we identify the folks in the back who will be answering questions, too?

Mr. WILSHUSEN. Ms. Melinda Dempsey, USAID. Mark Norman, who is the Audit Manager who has all the detail knowledge.

Chairman TOM DAVIS. Great. Thank you.

Mr. CRANDLEMIRE. Phil Heneghan, the Information Systems Security Officer, USAID.

Mr. DEFFER. Edward Coleman, my Security Director.

Chairman TOM DAVIS. Excellent.

Mr. ALVES. Rebecca Leng, Deputy Assistant Director.

Mr. MATTHEWS. This is Ed Densmore, Director of IT Security, Department of Transportation, and Dr. Dan Mehan who is the CIO of the Federal Aviation.

Chairman TOM DAVIS. You have enough help there, don't you?

And how about in the back? I just need to make sure the clerk gets everybody down for the record.

OK. Thank you.

[Witnesses sworn.]

Chairman TOM DAVIS. Thank you all very much for being here. We've got a 5-minute rule we try to follow. The goal is to get out of here about noon, so it will be 5 minutes apiece. So that leaves us time for questions and we'll be fine.

Your entire statement is in the record, so it will be based on that.

Mr. Crandlemire, we will start with you, and thank you for being with us today.

STATEMENTS OF BRUCE N. CRANDLEMIRE, ASSISTANT INSPECTOR GENERAL FOR AUDIT, U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT; JOHN STREUFERT, ACTING CHIEF INFORMATION OFFICER, U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT, ACCOMPANIED BY MARK NORMAN, USAID OIG; MELINDA DEMPSEY, USAID OIG; PHILIP M. HENEGHAN, USAID; FRANK DEFFER, ASSISTANT INSPECTOR GENERAL FOR INFORMATION TECHNOLOGY, U.S. DEPARTMENT OF HOMELAND SECURITY; STEVE COOPER, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY, ACCOMPANIED BY EDWARD G. COLEMAN, DHS OIG; TED ALVES, ASSISTANT INSPECTOR GENERAL FOR IT AND FINANCIAL MANAGEMENT, U.S. DEPARTMENT OF TRANSPORTATION; DANIEL MATTHEWS, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF TRANSPORTATION, ACCOMPANIED BY REBECCA LENG, DOT OIG; ED DENSMORE, DOT OIG; NATE CUSTER, DOT OIG; VICKI LORD, DOT OCIO; AND DR. DAN MEHAN, CIO, FAA

STATEMENT OF BRUCE N. CRANDLEMIRE

Mr. CRANDLEMIRE. Thank you, Mr. Chairman, and other committee members, for the opportunity to provide testimony for the U.S.

Agency for International Development's compliance with FISMA. As you requested, my testimony will focus on the state of information security at USAID and the methodology with which we used to perform our audit in 2004. In addition, I will discuss the need for standardized FISMA auditing framework and possibly what guidance would be needed for agencies to fully comply with FISMA.

USAID has made many positive strides over the last several years in addressing information security weaknesses. In particular, USAID has made several improvements in response to audits performed by my office and in turn substantially improved its computer security program.

In 1997, the Office of Inspector General identified information security as a material weakness at USAID; USAID information technology officials agreed with our conclusion and included it in USAID's annual report as required by FMFIA. At that time, USAID did not have an organizational structure that clearly delegated information security responsibilities, policies that provided for an effective information security program, or key management processes to ensure that security requirements were met. These material weaknesses remained outstanding for several years until fiscal year 2004, when USAID concluded, and we agreed, that information security was no longer a material weakness at the agency.

In the recent 2 years, the most significant changes are an appointment of an information security officer and the implementation of a centralized information security framework. Under this framework, USAID centrally manages its Windows 2000 domain servers, firewalls, and virus scan software for most of USAID's networks; instituted a process to assess information system security for the purchase of capital assets; and is continually updating its information security policies and procedures.

The agency has also identified several technological changes to improve its computer security. For example, they deployed Windows 2000, which has allowed the agency to lock down and configure security settings and incorporate many security improvements in comparisons with Windows 98. They have installed operating network sensors to detect unauthorized attempts to access our network. They run daily scans of its worldwide network to proactively identify potential vulnerabilities. They have also implemented a tips of the day program, which is an automated security awareness program that provides reminders to all system network users each day as a prerequisite to sign into the network.

Through these systemwide information technology and network changes, information security and information security awareness at USAID locations around the world have been significantly increased.

Although USAID has made substantial progress in improving security, information security weaknesses still remain. As reported in our 2004 FISMA audit report, the agency had not developed a disaster recovery program for its three major systems and had not tested the disaster recovery programs in two other systems.

The OIG methodology for assessing USAID information security into FISMA was to conduct an audit as opposed to an evaluation. For fiscal year 2004, our audit field work was conducted from Au-

gust 19th to October 6th and involved over 600 hours. In addition, as part of our financial statement audit, we incorporated about 2,800 staff hours as part of our general control work. This work complemented our FISMA work.

To perform the audit, we interviewed USAID officials to discuss their answers to the OMB questionnaire, and then we tested the support for the answers. For each of USAID's 49 answers to the questionnaire, we determined whether the agency's answer was supported by source documentation.

I am going to move now to the need for an Inspector General auditing framework for information security. In our opinion, since the OIG input to the FISMA process is used to upgrade security among civilian agencies, there is an implicit assumption that there must be a defined common set of attributes to facilitate meaningful comparisons of independent evaluation or audits performed by each IG.

Further, the establishment of these attributes or common security auditing framework should be developed on a collaborative basis among the IG community, OMB, and the Government Accountability Office. This framework also should address the resources needed to carry out the development and implementation of the framework along with congressional support for such an initiative.

I have just a couple comments on the existing process. I think the agencies and the IGs need more time to prepare or more time to respond to the annual FISMA questionnaire. Since 2002, the time between the issuance of the guidance until the time we actually start—we actually have to report in has gotten less. In 2002, it was 76 days, and this last year it was only 44 days. We need more time so we can more efficiently use our audit resources.

That concludes my statement.

[The prepared statement of Mr. Crandlemire follows:]

Office of Inspector General

Testimony of Bruce N. Crandlemire, Assistant Inspector General for Audit
U.S. Agency for International Development

Submitted to the Committee on Government Reform
U.S. House of Representatives

No Computer System Left Behind: A Review of the Federal Government's D+ Information Security Grade

April 7, 2005

Mr. Chairman and other Committee members:

Thank you for the opportunity to provide testimony on the U.S. Agency for International Development's (USAID) compliance with the Federal Information Security Management Act of 2002 (FISMA). As you have requested, my testimony will focus on the state of information security at USAID and the methodology we used to perform our fiscal year 2004 FISMA audit. In addition, I will discuss the need for a standardized FISMA auditing framework and what additional guidance is needed for agencies to fully comply with FISMA.

STATE OF INFORMATION SECURITY AT USAID

USAID has made many positive strides over the last few years in addressing information security weaknesses. In particular, USAID has made several improvements in response to audits performed by my office and, in turn, substantially improved its computer security program. Although there have been improvements in information security, USAID still faces several important challenges to refine its information security environment.

In 1997, the Office of Inspector General (OIG) identified information security as a material weakness at USAID. USAID information technology officials agreed with our conclusion and included it in USAID's annual report as required by the Federal Managers' Financial Integrity Act. At that time, USAID did not have (1) an organizational structure that clearly delegated information security responsibilities, (2) policies that provided for an effective information security program, and (3) key management processes to ensure that security requirements were met. This material weakness remained outstanding for seven years until fiscal year 2004 when USAID concluded, and we agreed, that information security was no longer a

U.S. Agency for International Development
1300 Pennsylvania Avenue, NW
Washington, DC 20523
www.usaid.gov

material weakness for the agency. As a result, information security at USAID today is a different story than it was in 1997.

In recent years two of the most significant changes are the appointment of an Information Systems Security Officer and the implementation of a centralized information security framework. Under this framework, USAID (1) centrally manages its Windows 2000 domain servers, firewall, and virus scan software for most of USAID's networks; (2) instituted a process to assess information systems security for the purchase of capital assets; and (3) is continually updating its information security policies and procedures.

The Agency has also initiated several significant technological changes to improve its computer security. For example, USAID has done the following:

- Deployed Windows 2000, which has allowed the Agency to lock down configured security settings and incorporated many security improvements in comparison to Windows 98.
- Installed operating network sensors to help detect unauthorized attempts to access USAID's network.
- Run daily scans of its worldwide network to proactively identify potential vulnerabilities in its network. Based on the results of the scans, the Agency's Information Systems Security Officer has been issuing monthly grades, similar to the grades listed in FISMA's annual report card, to its overseas missions.
- Implemented "Tips of the Day", which is an automated information security awareness program that provides security reminders to all system network users each day as a prerequisite to network login.

Through these system-wide information technology policy and network changes, information security and information security awareness at USAID's locations around the world have been significantly increased.

Although USAID has made substantial progress in improving information security, weaknesses still remain. As reported in our fiscal year 2004 FISMA audit report, the Agency had not developed disaster recovery plans for three major systems and had not tested disaster recovery plans for two other major systems. This represents a significant vulnerability because USAID is not fully prepared for an emergency event. To a lesser degree USAID also needs to:

- Improve its information resource management processes, such as the full implementation of information technology program management and oversight practices.
- Improve several management controls, such as outdated virus definitions, the installation of unauthorized software on employee computers, and the inconsistent updating of security software patches to individual computers.
- Test the effectiveness of USAID's security awareness program.

METHODOLOGY AND RESOURCES USED FOR THE FISMA AUDIT

The OIG approach to assessing USAID information security under FISMA was to conduct an audit as opposed to an evaluation. Our audit addressed all the reporting requirements of the Office of Management and Budget's (OMB) reporting template and the FISMA requirements.

In fiscal year 2004, the audit fieldwork was conducted from August 19 through October 6, 2004, and involved 610 staff hours. In addition, we relied on other audits (e.g., general control and Phoenix financial system audits) to support and compliment our FISMA fieldwork. For example, the fiscal year 2004 general control audit, which involved reviewing security controls of USAID's financial systems (in most cases, the same systems reviewed for FISMA), involved 2,843 staff hours. This audit included reviewing USAID's systems in Washington and at 12 overseas missions.

Our goal was to not only validate USAID's responses to OMB's questionnaire, but to also verify actions that USAID had taken to comply with FISMA. By verifying USAID's answers to OMB's reporting template, we could conclude where the Agency stood in terms of its compliance with FISMA.

Systems covered by the audit included the Washington financial system, the Missions financial system, the contract and procurement system, USAID's network system, and the Office of Foreign Disaster Assistance's network system. In addition to covering systems operated by USAID, we also determined whether the Agency had obtained security assurances for three systems operated by third parties: the payroll system operated by the National Finance Center, the letter of credit system operated by the Department of Health and Human Services, and the loan management system operated by Riggs Bank.

To perform the audit, we interviewed USAID officials to discuss their answers to OMB's questionnaire and then requested support for their answers. Types of source documents that we reviewed included: certification and accreditations for Agency and third party-operated systems, reviews of contractor facilities, reports to the United States Computer Emergency Team (USCERT) and internally generated security incident reports.

For each of USAID's 49 answers to the questionnaire, we determined whether the Agency's answer was supported by the source document provided and testimonial evidence. If an Agency answer was not supported, we brought that issue to management's attention. In the end, we agreed with 48 of the Agency's 49 answers. The one answer that we did not agree with involved whether the OIG had been included in the development and verification of the Agency's IT systems inventory.

NEED FOR AN INSPECTOR GENERAL AUDITING FRAMEWORK FOR INFORMATION SECURITY

In my opinion, since OIG input into the FISMA process is used to grade security among civilian agencies, there is an implicit assumption that there must be a defined common set of attributes to facilitate meaningful comparisons of independent evaluations/audits performed by each IG. Further, the establishment of these attributes or a common IG security auditing framework should be developed on a collaborative basis among the IG community (such as through the President's Council on Integrity and Efficiency forum), OMB and Government Accountability Office. Additionally, the framework should address the resources needed to carry-out the development and implementation of the framework along with Congressional support for such an initiative.

ADDITIONAL GUIDANCE, PROCEDURES, OR RESOURCES NEEDED TO IMPROVE COMPLIANCE WITH FISMA

In regards to OMB's FISMA questionnaire, there are two suggestions that we would like to make:

1. Agencies and IGs need more time to respond to the annual OMB FISMA questionnaire. Since 2002, time to respond to the questionnaire has decreased each year as follows:
    - In 2002, under GISR, OMB issued its guidance (M-02-09) on July 2 and expected responses by September 16—76 days.
    - In 2003, OMB issued its FISMA guidance (M-03-19) on August 6 and expected responses by September 22—47 days.
    - In 2004, OMB issued its FISMA guidance (M-04-25) on August 23 and expected responses by October 6—44 days.

2. The Office of Inspector General is responsible for conducting the FISMA audits at three micro-agencies: the Millennium Challenge Corporation, the African Development Foundation, and the Inter-American Foundation. OMB has established an abridged FISMA reporting format for micro-agencies (agencies with less than 100 Federal employees). While helpful, small agencies with more than 100 Federal employees struggle with responding to full FISMA requirements. This was noted by OMB in early 2005 and we understand that OMB is considering standardizing cyber security business processes of agencies to save money, increase security, and help those agencies with small IT budgets. In the future, OMB might want to consider not just employee numbers, but also IT budgets in its definition of micro-agencies (e.g. agencies with less than 250 employees and IT budgets less than a certain dollar threshold).

SUMMARY

In summary, USAID has made positive strides in addressing information security weaknesses, and our audits have confirmed the improvements. Although there is still work to be done, USAID is on the right path.

Again, thank you for the opportunity to testify today. I will be happy to respond to any questions you may have.

Chairman TOM DAVIS. Thank you very much.

Mr. Streufert, thanks for being with us.

STATEMENT OF JOHN STREUFERT

Mr. STREUFERT. Thank you, Mr. Chairman, and members of the committee. I want to thank you for the opportunity to testify on the status of our FISMA implementation and our security program. We submitted detailed information in response to your questions. What I would like to do in my oral remarks is address the 10 reasons that helped us improve our IT scores during the past period.

No. 10, our industry partnerships. USAID has teamed with industry both in services and in our tools to increase performance. There has been a commitment to continuous improvement that has now spread over a 2-year period.

No. 9, managing risk. Our agency information system security officer defined risk as critical. We want to be compliant with the rules but make sure that compliance does not overshadow our responsibility to attend to threats and impact on our business results.

No. 8, central administration. USAID IT security sensitive settings have been drawn from 80 countries and 20 time zones to be administered centrally at AID headquarters. This would not have happened without executive support at all levels. We have one organization and one approach when it comes to security.

Continuous awareness. As Bruce mentioned, we have a product called tips of the day implemented worldwide where 135,000 instances of training and awareness came into effect. Our awareness also includes the followup on every action item we have of a finding of a security improvement.

Item 6, rules of behavior. The agency has defined that the use of the network and our systems is a privilege and not a right. Though our employees have overwhelmingly supported IT security for the imperative it is, a handful of employees who have violated IT rules of behavior have been submitted for disciplinary action and, where warranted, recommended for removal for the reasons of that improper conduct.

Continuous measurement. USAID has 15,000 devices connected to it worldwide, 5,000 software tools and packages, 8 major applications and 3 what we call general support systems against which our disciplines are applied. These devices are centrally checked worldwide 10 times a month for among 33,000 possible IT security weaknesses using the same tool that protects worldwide international credit card transactions. We felt that the most sophisticated tool was in fact important for our purposes.

Management accountability, to refer to an item one of the members drew attention to. We give the boss of our 90 technical managers worldwide a grade of A to F once a month, because it is their business at risk in addition to ours collectively. Regions and bureaus who represent these 90 technical managers and their bosses receive grades A through F for all their reporting units, which has created a competition for excellence. Our managers have performed this work in harm's way, Afghanistan, Iraq, and other hardship posts, and among operating environments where power and other circumstances such as interrupted telecommunication lines have

made it difficult. Notwithstanding these difficulties and including setting up for tsunami relief, we have been able to implement a security program and found significant benefits for it.

Item No. 3, correlation of threats. We have found it essential to install sensors throughout our networks to capture those critical events and submit them to a statistical correlation so that we may find whether systematic attacks in fact are occurring which otherwise would be hidden from visual inspection.

Item No. 2, continuous audit review. We have forged over the past 7 years a partnership with our Inspector General who has in fact audited every significant IT initiative of our organization for the past 7 years. We have come to learn that the harshest criticism from our auditors and others, GAO and externally, is a source for building on strength, and we have chosen to respond to those items of improvement in just that way.

Last and perhaps most importantly, our Administrator Andrew Natsios defined IT security as critical to success of the agency. He has defined the need to improve management systems across the board, and information technology was one of those areas of improvement. In each of the cases where a critical issue was facing the agency in the area of IT security, when we carried it forward to him we received his full support. We believe the correct decisions were made, which in fact has been critical to the success of our organization and our security effort.

Thank you very much.

[The prepared statement of Mr. Streufert follows:]

TESTIMONY OF JOHN STREUFERT,
ACTING CHIEF INFORMATION OFFICER,
U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT (USAID)
BEFORE THE HOUSE COMMITTEE ON GOVERNMENT REFORM ON THE STATUS OF FEDERAL AGENCIES' IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002
April 7, 2005

Chairman Davis and Members of the Committee, I want to thank you for the opportunity to testify on the status of USAID's Information Systems Security Program and our implementation of the Federal Information Security Management Act (FISMA). We appreciate your interest, and look forward to close cooperation with you and your committee as USAID continues to improve our Information Systems Security Program.

I would like to begin by describing USAID's mission and the unique information system security challenges created by this mission. Then I would like to report to you on how our risk-based Information Systems Security Program has successfully implemented FISMA. Lastly, I will provide a recent example of how this risk-based approach allowed USAID the flexibility to respond to the December 2004 tsunami.

USAID's Unique Mission Drives Our Information Systems Security Program

USAID was created as an independent agency in 1961 by the Foreign Assistance Act. Since that time, USAID has been the principal U.S. agency to extend assistance to countries recovering from disaster, trying to escape poverty, or engaging in democratic reforms. USAID fosters long-term and equitable economic growth and advances U.S. foreign policy objectives by supporting: economic growth, agriculture, and trade; global health; and democracy, conflict prevention, and humanitarian assistance.

Our headquarters is here in Washington, D.C., with field offices in more than 70 countries around the world. To achieve our mission, USAID works in close partnership with many different Private Voluntary Organizations (PVOs), indigenous organizations, universities, American businesses, international agencies, other governments, and Non-Governmental Organizations (NGOs).

USAID's mission requires us to work in developing countries; this creates many challenges for implementing a worldwide Information Systems Security Program. The information technology and telecommunications infrastructure in most of the countries where USAID does its work are not as robust or dependable as the infrastructure here in the United States. Yet, work with our development partners compels us to work with and

be part of this developing infrastructure. Some of the information technology infrastructure challenges in these developing countries include: unreliable power grids, non-existent fiber optic connections, expensive bandwidth, and high latency. Furthermore, we rely on locally trained staff to manage USAID's systems at each of our field offices as well as to provide help desk support to the 6,000 workstation users in our field offices around the world.

This means that the risk environment in which USAID operates is unique.

Although USAID operates three separate computer networks (each supported by a different risk model), most of the USAID information technology activity occurs on AIDNET, which is a single worldwide network made up of 8,000 interconnected workstations and 7,000 other network infrastructure devices. Approximately 2,000 of the workstations are here in Washington with the remaining 6,000 workstations located in more than 70 countries around the world.

AIDNET is a very active network. We receive approximately 2 million emails a month and block the 500,000 of those emails that are spam. We also block more than 150,000 viruses each month. USAID's firewalls are located at more than 50 sites around the world but are managed and controlled in Washington, D.C. The firewalls handle more than 11 million access attempts each day and deny 4 million of those attempts. We have approximately 36,000 web pages on our public web site and 20,000 web pages on our intranet. The public pages are accessed more than 6 million times a month and the internal pages are accessed more than one million times a month.

Risk-Based Program to Protect the Confidentiality, Integrity, and Availability of USAID Information Resources

Our Information Systems Security Program uses a risk-based management model that requires us to support our business decisions with information security metrics. To support this model, we focus on computer security awareness. We deploy security data collection technology to provide risk measurements. We report this information to

agency business system owners and decision makers in near real-time. These technologies provide us in-depth visibility into the daily operations of our global network and increase security awareness among USAID managers and staff. This risk-based approach is the only model with which we feel USAID can meet the challenges of today's dynamic security landscape. I would now like to discuss some of these technologies specifically and describe how each supports our risk-based approach to managing information security.

USAID uses an automated, daily security awareness tool called Tips of the Day to deliver training to employees and contractors worldwide. Every day during user login, the tool provides a brief lesson on computer security and then poses a security question that the user must answer to complete the login process. The tips are generated randomly for each individual, so typically our users do not receive the same tips. Last year we completed the worldwide deployment of the Tips of the Day program, and we were able to produce accurate metrics on the actual number of employees receiving this training. During fiscal year 2005 we will begin grading the user responses and reporting those grades to agency managers. These daily tips achieve precisely the results desired from awareness training – they reinforce the importance of computer security at USAID. Every user, including senior management, receives this daily computer security awareness training. Information security awareness, at all levels of USAID, is the foundation on which our Information Systems Security Program is built, and we plan to continue enhancing and improving our computer security awareness program.

If awareness training is the foundation, an important pillar of our Information Systems Security Program is vulnerability management. By understanding our vulnerabilities, we can measure the amount of risk we accept on a day-to-day basis. Our vulnerability management software continually scans our network (24 hours a day, 7 days a week). The 15,000 devices on our network are scanned, on average, 10 times a month. This scanning provides a continually updated status of our vulnerability posture to system managers and Information Systems Security Officers. In addition, we have developed a monthly grading system to help senior managers better understand their risk posture. We report these grades each month, on an A to F scale, to more than 90 system and

application owners (these owners are senior managers in USAID). We also send executive summaries to the bureau heads and other senior managers in USAID. For example, we provide an Africa regional report to the Assistant Administrator for the Africa Bureau. This report summarizes all mission information systems security vulnerabilities and allows the bureau to determine needs for resource allocations. We also provide the Chief Financial Officer with monthly reports grading the security of all the systems around the world that are running major financial applications. Our capability to accurately measure and report in a timely manner the vulnerability status of our systems has been an effective method of managing our information systems security. Over the last twelve months we have significantly reduced the enterprise vulnerability posture; this is reflected in the grades provided to managers. The overall vulnerability assessment grade for the agency as an enterprise has moved from a C to an A.

Even though we have reduced our network-based vulnerabilities, we understand that security is a moving target. We cannot mitigate all the risks any more than we can stamp out all the possible vulnerabilities. Network threats exist. To combat this reality, we have deployed a global network of security devices that transmit security event information to a central collection, correlation, and reporting system called a Security Information Management system (SIM). This SIM collects suspicious security events and anomalies from hundreds of security devices and firewalls deployed throughout the enterprise. By collecting all our security events in the SIM database, we are able to correlate events across all disparate security device types within the enterprise, a powerful and critical tool when managing incident response on a global network. With daily reviews and active monitoring, we can identify and quickly respond to new information technology security threats and virus attacks. The technology also supports our incident reporting to US-CERT at the Department of Homeland Security, which provides important information to the rest of the federal community.

USAID has completed the certification and accreditation of all our major applications and systems. The certification and accreditation process used by USAID provides a regular and recurring review of all our major applications and systems. The certification of major applications and systems is done through my office by the USAID

Information System Security Officer (ISSO) which ensures that all major information technology investments receive a consistent view of risk information.

Part of the role of the Information Systems Security Officer is to make sure that the business system owners understand all the identified risks and the resource requirements associated with implementing the planned mitigation strategies. System accreditation is the responsibility of the business system owner. Who better understands the business requirements, what risks may be acceptable, or whether it is more cost-effective to mitigate a risk with a manual control than the business owner supporting the investment? In our experience, business owners, when they understand the risks, apply their resources to effectively mitigate and manage the identified risks.

The accreditation process requires the business owner to determine if the residual risk to agency operations, agency assets, or individuals is acceptable. If the risk is acceptable, an authorization to operate the system is issued and a plan of action and milestones for mitigating any residual risks is established. The Plan of Action and Milestones for each investment informs the USAID's Capital Planning and Investment Control (CPIC) committee of the current risk posture of the agency's steady state investments. This process provides a mechanism for the CPIC to consider security and risk factors before making investment funding decisions. USAID's Business Transformation Executive Committee serves as the Agency's CPIC authority.

How the USAID Risk-Based Approach Allowed USAID to Respond to the Recent Tsunami

Allow me to provide a recent important example of our risk-based approach to information security and how this approach supported USAID decision-making to quickly respond to the needs of those affected by the tsunami. As you know, USAID has the responsibility for managing the U.S. Government's response to natural disasters that occur around the world. Internally, this effort is managed by USAID's Office of Foreign Disaster Assistance (OFDA). OFDA's work environment is very

different than that of the programmatic bureaus in the Agency that typically work on long-term development projects in our field offices overseas. OFDA must respond quickly to disasters that occur anywhere in the world. It must be mobile and agile to respond to emergencies in remote areas. OFDA's response teams operate at the site of the emergency and do not always operate from USAID's field offices.

As a result, the OFDA network uses a risk model different than AIDNET. The OFDA risk model stresses the importance of system availability over system confidentiality. This model allows OFDA to pre-position and pre-deploy systems to ensure rapid response to disasters and emergencies anywhere in the world.

Because of the different OFDA risk model and operational requirements, USAID created a network called OFDANET that is separate from AIDNET. In FISMA parlance, OFDANET is a separate General Support System (GSS) with its own Certification and Accreditation.

In December 2004, OFDA was called upon to provide relief in countries that were devastated by the tsunami. In responding to this disaster, OFDA quickly deployed Disaster Assistance Response Teams (DARTs) to the affected areas using computers and laptops that had been pre-positioned in Asia. With the OFDA computers in place, these teams were able to begin assessments and move funds to provide food and medical supplies to the needed areas immediately.

However, the enormous scale of this disaster also required that our USAID missions in this region rapidly add staff and computers to support the long-term rebuilding efforts. For example, the USAID mission in Sri Lanka, one of the hardest hit areas, added dozens of new computers to AIDNET. Our system administration staff, led by systems manager Anil Liyange, worked around the clock to provide the information systems infrastructure to support the United States government relief efforts in the region. Our other missions in the affected areas also needed to expand the number of workstations on their networks as well.

Any time there is an unplanned increase in the number of systems connected to the network, additional risk is introduced. Because USAID continually measures the system risks to its enterprise, we were able to make an informed and rational decision to allow this rapid, unplanned expansion of AIDNET and accept the added risk in order to meet our emergency business requirements. Further, we could report and track this risk until mitigated to an acceptable level.

In this instance, a compliance-based approach to information security may have hindered our ability to respond to the tsunami. Despite the differences between the AIDNET and OFDANET risk models, USAID's Information Systems Security Program promotes secure business decisions. This risk-based approach enables us to meet our FISMA responsibilities and enhances our ability to accomplish USAID's mission.

In summary, USAID's mission presents unique information security challenges. We have responded to these challenges by establishing a risk-based Information Systems Security Program that emphasizes computer security awareness, and deploys technologies to continually measure and report risk to the business and program executives. We will continue to adapt and improve our program as new regulatory guidance is published and as new security and information system technologies are developed. Our Information Systems Security Program enables USAID to work in a unique environment while protecting the confidentiality, integrity, and availability of USAID information resources.

I appreciate the opportunity to appear before you today and I would be pleased to answer any questions that you may have.

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

STATEMENT OF FRANK DEFFER

Mr. DEFFER. Thank you, Mr. Chairman, and members of the committee, for the opportunity to be here today to discuss the status of FISMA implementation in the Department of Homeland Security.

Mr. Chairman, I would note at the outset that we in the Inspector General's office have developed an effective working relationship with the DHS CIO and his staff in order to facilitate FISMA compliance at DHS.

As we reported last year, DHS has made significant progress in developing and implementing its information security program at the headquarters level. For example, DHS developed the necessary plans such as the information security program management plan to provide the foundation for an agencywide program. Based on our review of those plans, DHS has established an adequate structure, blueprint, and process to implement and manage its program. Also, the Department has developed an adequate process to report security weaknesses in its plan of action and milestones, or POA&M, and has adopted an enterprise management tool, trusted agent FISMA, to collect and track data related to all POA&M activities.

Even with these efforts, however, there are a number of factors that are hindering further progress. Specifically, one of the impediments to implementing DHS's program is that the CIO is not a member of the department's senior management team. Therefore, the CIO does not have the authority to strategically manage agencywide IT programs, systems, or investments. Furthermore, there is no formal reporting relationship between the DHS CIO and the component CIOs or between the DHS CISO and the department security managers.

Also, DHS does not have an accurate and complete system inventory. An initial attempt at developing an inventory in 2003 did not provide an accurate picture of DHS's information systems. In September 2004, DHS began a second effort using an outside contractor to establish a system inventory.

Finally, while DHS has developed an adequate process to report security weaknesses in its POA&M, DHS components have not established verification processes to ensure that all IT security weaknesses are included. Overall, DHS is on the right track to create and maintain an effective program. However, the Department and its components still have much work to do to become fully FISMA compliant.

Mr. Chairman, as you know, annual information security evaluations began 4 years ago with the Government Information Security Reform Act [GISRA]. And I would say that, after being involved in four of these efforts, two at the State Department OIG, and using a different approach each time, it is becoming clear that a more standard approach is needed, perhaps similar to that used in financial audits. This standard framework would ensure—help ensure that all IGs review and report on the same information across all agencies. Currently, each IG performs its FISMA evaluation based on its interpretation of FISMA and OMB guidance. A standard

audit framework should allow OMB and Congress to more effectively and objectively determine the status of information security across the entire Federal Government.

Finally, let me say a few words about what additional guidance or procedures are needed to help improve FISMA compliance. OMB issues annual guidance to agencies and IGs to promote consistent reporting across government and to ensure that agencies comply with FISMA. But this guidance needs to be clearer. For example, organizational components in DHS have struggled with the definition of a system for FISMA reporting. This has hindered DHS's ability to develop a reliable inventory.

Another area of concern is how security of systems is measured by the FISMA metrics. OMB asks the agencies and IGs for the number of systems that have been reviewed, certified, and accredited, but treats all systems the same. That is, systems are not differentiated between routine or mission critical. For example, an agency may have certified and accredited 80 percent of its systems, but it could still be seriously at risk if its mission critical systems are those that have not been certified and accredited.

Mr. Chairman, this concludes my prepared statement. I appreciate your time and attention, and welcome any questions from you or members of the committee.

[The prepared statement of Mr. Deffer follows:]

STATEMENT OF FRANK DEFFER

ASSISTANT INSPECTOR GENERAL, INFORMATION TECHOLOGY AUDITS

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

APRIL 7, 2005

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to be here today to discuss the status of the implementation of the Federal Information Security Management Act of 2002 (FISMA) within DHS. My testimony will address: the state of information security at DHS; the methodology and the resources used to evaluate the information security program at DHS; whether there is a need for a standard IG auditing framework for information security; and, whether additional or modified guidance is needed to improve compliance with FISMA. This testimony does not include the status of FISMA as it relates to intelligence systems. I would be happy to brief you on that issue at a later date.

DHS' Information Security Program

DHS developed an Information Security Program Strategic Plan, dated April 4, 2004 to provide the foundation for an agencywide, consolidated information security program. Under this plan, DHS' Chief Information Officer (CIO) and Chief Information Security Officer (CISO) identified eight security program areas:

- Management and Integration
- Security Policy
- Security Operations
- Security Architecture
- Continuity Planning
- Compliance and Oversight
- Training, Education, and Awareness
- National Security Systems and COMSEC

These distinct security program areas comprise the framework of the department's security program. The strategic plan describes the goals and objectives for establishing a dynamic information security organization over the next five years, too. We believe the program areas established in this plan represent key segments necessary for an effective information security program.

DHS' CIO, who has oversight responsibilities for the information security program, delegated the CISO, as required under FISMA, the authority to establish information security policies and procedures throughout the department. In June 2004, the CISO developed the Information Security Program Management Plan, which is the blueprint for managing DHS' information security program. At the same time, the CISO developed an Information Security Risk Management Plan, which documents DHS' plan to develop, implement, and institutionalize a risk management process in support of its information security program. Based on our review of these plans, DHS has established an adequate structure, blueprint, and process to implement and manage its information security program.

Additionally, the CISO developed and issued baseline IT security policies and procedures in a management directive; and a Sensitive Systems Policy Publication and its companion, the Sensitive Systems Handbook as well as a National Security Systems Policy Publication and its companion, the National Security Systems Handbook. While the guidance issued adequately documents key information security policies and procedures, there is additional guidance that needs to be either strengthened or developed to help DHS and its organizational components implement and maintain an effective information security program. Areas where additional guidance is needed include:

1) wireless technologies according to NIST SP 800-48;
2) protecting critical infrastructures from cyber vulnerabilities and threats;
3) remote access to DHS' systems;
4) vulnerability scanning;
5) penetration testing;
6) incident detection, analysis, and reporting;
7) security configuration policies and procedures;
8) specialized security training; and,
9) IT security training costs.

The department has developed an adequate process to report and capture known security weaknesses in its Plan of Action and Milestones (POA&M) and has adopted an enterprise management tool, *Trusted Agent FISMA*, to collect and track data related to all POA&M activities. *Trusted Agent FISMA* is used to collect data on other FISMA metrics, too. Last, the department purchased a certification and accreditation tool that will be used by all components to certify and accredit all systems.

Each organizational component has appointed an Information Systems Security Manager (ISSM) to ensure that the component's information security requirements are properly implemented, managed, and enforced; and, that its information security program is aligned with the DHS Information Security Program. DHS' CISO issued guidance, in the *ISSM Guide to the DHS Information Security Program* (dated July 19, 2004), to the organizational component's ISSMs which outline specific responsibilities. Together, the policies and procedures developed by the DHS CIO and CISO - when fully implemented by the components - should provide DHS with an effective information security program that complies with FISMA.

While DHS has made significant progress over the last two years to develop, manage, and implement its information security program, its organizational components have not yet fully aligned their respective security programs with DHS' overall policies, procedures, or practices.

Factors which kept the department from having an effective information security program include lack of a system inventory, lack of a formal reporting structure between the CIO and the organizational components, and lack of a verification process for FISMA performance metrics including security weaknesses.

- One of the impediments to implementing DHS' agencywide information

security program is that the CIO is not a member of the department's senior management team. Therefore, the CIO does not have the authority to strategically manage agencywide IT programs, systems, or investments. Furthermore, there is no formal reporting relationship between the DHS CIO and the component CIOs or between the DHS CISO and the organizational components' ISSMs. While DHS' CISO meets with the ISSMs on a regular basis and has issued departmental security policies and procedures, he does not have the authority to oversee or ensure that the organizational components' management of their information security program complies with DHS' agencywide security program policies and procedures.

- DHS does not have an accurate and complete system inventory. An initial attempt at developing a system inventory in FY 2003 did not lead to an accurate picture of DHS' information systems. The lack of understanding by those responsible for identifying required system information has hindered DHS' ability to compile a comprehensive system inventory. In September 2004, DHS began a second effort using an outside contractor to establish an agencywide system inventory. A standard methodology for identifying the inventory at each organizational component was developed and the department hopes to complete this task by the end of the summer. Once the inventory is complete, the department should be positioned to better manage its critical systems.

- While DHS has developed an adequate process to report and capture known security weaknesses in its Plan of Action and Milestones (POA&Ms), DHS' organizational components have not established verification processes to ensure that all known IT security weaknesses are included in POA&Ms. With no assurance that all security weaknesses have been identified, DHS cannot verify that all security weaknesses are mitigated or corrected.

- Finally, due to the lack of resources in the DHS CISO office, there has been a limited effort devoted to verifying FISMA metrics as reported by the organizational components. Until the CISO can determine with confidence the FISMA metrics for its components, DHS cannot effectively manage its information security program.

Overall, DHS is on the right track to create and maintain an effective information security program. However, the department and its components still have much work to do to get to the point where DHS has a mature FISMA compliant information security program.

Methodology and Resources Used to Audit DHS

The Information Security Audit Division, within the Information Technology Audit group is responsible for assessing the security of information systems and for conducting the annual FISMA evaluation. We performed the 2004 FISMA evaluation utilizing the requirements outlined in OMB Memorandum M-04-25, *FY 2004*

Reporting Instructions for the Federal Information Security Management Act. We conducted our fieldwork at the program level (DHS CISO) and at DHS' major organizational components. We assessed DHS' compliance with the security requirements mandated by FISMA and other federal information systems security policies, procedures, standards, and guidelines; including NIST SP 800-26 (*Security Self-Assessment Guide for Information Technology Systems*) and NIST SP 800-37 (*Guide for the Security Certification and Accreditation of Federal Information Systems*).

Specifically, we used the previous year's FISMA independent evaluation as a baseline for our evaluation and assessed the progress that DHS and its organizational components have made in resolving weaknesses previously identified. We reviewed DHS' Plan of Action and Milestones (POA&M) process to determine whether all security weaknesses were identified, tracked, and addressed. We identified the policies, procedures, and practices that DHS has at the program level as well as at the organizational component level. We evaluated the processes, such as certification and accreditation, security training, and incident response, that DHS has implemented as part of its agencywide information security program.

We utilized contractors to test DHS' compliance with NIST security guidance for a sample of eight systems at seven organizational components to ensure that weaknesses, if any, were identified, captured, and tracked in the POA&Ms. Contractors were used to evaluate DHS' major organizational components progress in developing, aligning, and managing their information security program and practices in compliance with the agencywide information security program. Areas that were reviewed included information security awareness training; security incident detection, handling, response and reporting; certification and accreditation; security configuration management; and, POA&Ms.

Additionally, we included in our FISMA responses the results of audits which were performed during the reporting period - including the financial statement audits, and information security audits of wireless networks, remote access systems, and national security systems. Our ongoing audit work will allow us to determine how the department and its components are managing and securing its information systems. For example, we are currently performing audits of network security, database security, and the major DHS application - US-VISIT.

Need for a Standard Information Security Audit Framework

There is a need for a standard audit framework for information security similar to that used in financial audits. This framework would help ensure that all IGs review and report on the same information across all agencies. At this time, each IG performs its FISMA evaluation based on its interpretation of FISMA and OMB guidance. The extent and depth of the FISMA evaluation also is based on the resources that are available to perform the review. A standard audit framework should allow OMB and Congress to more effectively and objectively determine the status of information security across the entire federal government. A standard audit framework would help

the agencies, OMB and Congress to determine the progress each agency is making in improving or maintaining its information security program.

Additional Guidance and Procedures Needed to Comply with FISMA

OMB issues annual guidance to agencies and IGs to promote consistent reporting across government and to ensure that agencies comply with FISMA. However, clearer guidance would assist agencies and IGs in helping to ensure that all federal agencies comply with and report on FISMA.

One suggestion is to establish a standard "cut-off" or "as-of" date to perform the annual agency assessment and IG independent evaluation, similar to the fiscal year-end used for financial statement audits. The cut-off date should be one-two months prior to the report's due date to OMB. By establishing a fixed date, agencies and IGs would have adequate time to review the information security programs and respond to OMB. Any security program improvements made after the cut-off date would be addressed in the next year's FISMA report. A cut-off date would allow for consistency among agency reports since all reports would cover the same period of time. Further, if OMB requests that IGs evaluate the agency's FISMA responses, the IGs reports should be due at least one month after the agency's FISMA report is due. This would allow the IG to evaluate the agency's responses to the FISMA metrics and questions and obtain responses to any recommendations.

The timing of the OMB issuance of the guidance needs to occur sooner in the year. Each year the final guidance is issued closer to the date the FISMA report is due to OMB. Last year, for example, OMB did not issue its final guidance until August 23, 2004 - when the final report was due to OMB October 6, 2004. In the previous year, the final guidance was issued on August 6, 2003 and in 2002 the guidance was issued on July 2, 2002. Such late issuance of the reporting instructions does not allow the CIOs or IGs to effectively collect all program measures required by OMB throughout the year. Since there is little time to address the additional and changed performance measures from the previous years' reporting requirements, the IG may need to reallocate resources to determine the status of these performance measures very quickly in order to complete the FISMA report timely. Additional performance measures that were requested last year included determining if the agencies had begun assessing systems for E-authentication risk; determining the policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training; determining if agency wide policies that require specific security configurations have been implemented and the degree by which the configurations have been implemented; and determining the overall quality of the certification and accreditation process.

Also, DHS' organizational components have struggled with the definition of a "system" for FISMA reporting. Since the DHS CISO has been unable to rely on the number of systems reported by the components, the CISO cannot properly manage the information security of all critical systems. Other areas where the department has struggled with definitions in the FISMA guidance include contractor services and the role that the agency has in overseeing the security of the contractor as well as the

difference between significant deficiencies, material weaknesses, and reportable conditions as they relate to FISMA reporting.

Another area of concern is how security of systems is measured by the FISMA metrics. OMB asks the agencies and IGs for the number of systems that have been reviewed, certified, and accredited but treats all systems the same. That is, systems are not differentiated between routine or mission-critical systems. For example, an agency may have certified and accredited 80% of its systems, but it could still be seriously at risk if its mission-critical systems are those systems that have not been certified and accredited.

An area where modification to the OMB guidance would be helpful to the IGs and does not appear to be a benefit in reporting is the requirement for the IGs to fill out numbers in some of the tables (i.e., system inventory, incident reporting and analysis, training) that are already reported by the agency. Since the guidance only requires that the IGs report on systems that they have reviewed or information that they have verified, there does not appear to be any benefit in reporting these numbers for larger agencies.

Mr. Chairman, this concludes my prepared statement. I appreciate your time and attention and welcome any questions from you or Members of the Committee.

Related DHS OIG Information Security Audit Reports

- DHS Information Security Program Evaluation, FY 2003
  (OIG-IT-03-02, September 2003)
- Evaluation of DHS' Information Security Program for Fiscal Year 2004
  (OIG-04-41, September 2004)
- Inadequate Security Controls Increase Risks to DHS Wireless Networks
  (OIG-04-027, June 2004)
- Progress and Challenges in Securing the Nation's Cyberspace
  (OIG-04-029, July 2004)
- DHS Need to Strengthen Controls for Remote Access to Its Systems and Data
  (OIG-05-03, November 2004)
- DHS Requires Additional Processes and Controls Over Its National Security Systems
  (OIG-05-09, January 2005)

Chairman TOM DAVIS. Thank you very much.

Mr. Cooper, I understand that you announced today, at least from reading the trade press, that you are leaving your post.

Mr. COOPER. I did.

Chairman TOM DAVIS. I just want to say—well, I hope this isn't your last time before the committee; we may bring you back as a consultant, but we appreciate the job that you have done.

Mr. COOPER. Thank you.

Chairman TOM DAVIS. You have been steadfast in coming before us and offering your ideas, and we consider you a valuable asset to the committee. Thanks for being with us.

STATEMENT OF STEVE COOPER

Mr. COOPER. Thank you, Mr. Chairman, and members of the committee. It is my pleasure to appear before the committee again, and I wish to thank the chairman and the members for providing me the opportunity to update you on our efforts and progress in integrating and securing information systems within the Department of Homeland Security.

I would like to begin by acknowledging the important role that our Inspector General plays in the Department. We have established an extremely effective and collaborative partnership with our Inspector General, and especially with respect to the development and operations of information technologies and support of the critical missions of the Department. The IG has been an important and independent voice as the Department formulates a strategy for building a robust and effective information security program.

Mr. Deffer has provided what I believe to be an accurate and detailed assessment of our progress to date and rather than repeat what has been already said I would like to focus my remarks on the future.

The DHS Information Security Program is structured around compliance with FISMA as well as OMB and NIST guidance. I want to stress that we are not proud of our failing grade. We have done much, and much needs to be done. Specifically, we have implemented and continue to implement a number of security performance metrics to address the issues represented by the FISMA grade.

I fully understand that the success of the Department is dependent upon our ability to protect sensitive information used to secure the homeland, and to this end, the Department's Information Security Program has been designed to provide a secure and trusted computing environment based upon sound risk management principles and program planning. The development of a formal trust model within this program will eliminate institutional barriers that regularly divide organizations and will enable disparate agencies to more effectively share information within this common trusted framework. We have implemented a digital dashboard that provides us for the first time with the status of security performance based upon computed FISMA metrics, and we have implemented a security performance scorecard.

Three key Information Security Program initiatives under way for over a year now are beginning to provide tangible results. As these three efforts converge, together they will pave the way for

real and measurable security improvements in the near future. These include, first, completing a comprehensive baseline inventory for defining accreditation boundaries and assigning responsibilities for security controls for appropriate program officials throughout the Department; second, fielding a robust set of automated enterprise security management tools to optimize our security processes; and, third, implementing a comprehensive and repeatable set of metrics for holding program officials accountable.

The baseline systems inventory project now under way has already identified a significant number of legacy systems that were not previously identified in our initial systems inventory that we did during the standup of the Department. At one of the organizational elements, this most recent system inventory project has now identified 106 information systems programs compared to the 5 that were previously identified at standup.

In response to this legacy issue, the Department is developing a comprehensive remediation plan for completing all the required certification and accreditations by the end of fiscal year 2006. Related to these actions, we have implemented a department plan of action and milestones process and an enterprised system to manage that plan of action. Evidence that DHS is successfully institutionalizing this process is demonstrated by the fact that our initial fiscal year 2003 program and milestones contained less than 100 line items, meaning task activities that we identified that we needed to do, while our current plan now contains several thousand line items and activities.

Furthermore, we have implemented a certification and accreditation tool that will ensure C&A equality and map that certification and accreditation testing to our established policies. The C&A and remediation plan will include a prioritized list of systems to be certified based upon the system's security impact level, which means the systems with higher security impact levels will be the first systems that we will accredit if not already accredited. This remediation plan will identify a variety of funding alternatives for completing all certifications and accreditations, and our new automated security management tools are already designed to streamline this process. Use of this tool has now been mandated for all activity initiated after April 10th.

This aggressive remediation effort will provide a sound baseline of secure systems with appropriate controls in place. However, we must continue to improve our security posture throughout the life cycle of each and every system or application in use in the Department. For this reason, we are continuing to refine the program so that we will remain relevant for the future. Program enhancements currently under way include developing a communications plan for our information security program, to include a Web-based information security portal that will improve the availability of information security data to all DHS employees, including those who do not have access to DHS Online; and, publishing an updated Information Security Program strategic plan outlining a revised vision for the future of the program based on lessons learned over the past 2 years.

Finally, to sustain a viable and healthy information systems program and security program, I know that we must have strong sup-

port throughout the Department. Through the DHS Chief Information Officers' Council, I will work with each member to ensure that we not only continue to improve our security posture through periodic program reviews, but that we also implement new and improved measures wherever appropriate.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Cooper follows:]

Information Security Statement by
Steven Cooper
Chief Information Officer
U.S. Department of Homeland Security
Before the
U.S. House of Representatives Committee on Government Reform

Thursday, April 7, 2005

Mr. Chairman and Members of the Committee:

Good morning, I am Steve Cooper, Chief Information Officer for the Department of Homeland Security (DHS). It is my pleasure to appear before the Committee and I wish to thank the Chairman and Members for the providing me the opportunity to update you on our efforts and progress in integrating and securing information systems within the Department.

I would like to begin by acknowledging the important role our Inspector General (IG) plays in the Department, and especially with respect to the development and operations of information technologies in support of our mission. The IG has been an important and independent voice as the Department formulates a strategy for building a robust and effective Information Security Program. Mr. Coleman has provided what I believe to be an accurate and detailed assessment of our progress to date, and rather than repeat what has already been said, I would like to focus my remarks on the future.

The DHS Information Security Program is structured around compliance with the Federal Information Security Management Act (FISMA), as well as Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) guidance. Our primary focus is to enable effective and secure information sharing. I want to stress that we are not proud of our failing grade. We have done much, and much needs to be done. Specifically, we have implemented and continue to implement a number of security performance metrics to address the issues brought up in the FISMA grade.

I fully understand that the success of the Department is dependent on our ability to protect sensitive information used to secure the homeland; and, to this end, the Department's Information Security Program has been designed to provide a secure and trusted computing environment based on sound, risk-management principles and program planning. The development of a formal trust model within this Program will eliminate institutional barriers that regularly divide organizations, and will enable disparate agencies to more effectively share information within a common trusted framework. We have implemented a Digital Dashboard that provides the status of security performance based on computed FISMA metrics and we have implemented a security performance scorecard.

Three key Information Security Program initiatives, underway for over a year, are now

providing tangible results. As these three efforts converge, together they will pave the way for real and measurable security improvements in the near future. These include:

(1) Completing a comprehensive base-line inventory for defining accreditation boundaries and assigning responsibilities for security controls to appropriate Program Officials throughout the Department,

(2) Fielding a robust set of automated enterprise security-management tools to optimize our security processes; and,

(3) Implementing a comprehensive and repeatable set of metrics for holding Program Officials accountable.

The base-line systems inventory project now underway has already identified a significant number of legacy systems that were not previously included in the initial system inventory developed during the standup of the Department. At one of the Organizational Elements, the system inventory project has now identified 106 information systems compared to the five systems that were previously identified at stand-up.

In response to this legacy issue, the Department is developing a comprehensive remediation plan for completing all the required Certification and Accreditations (C&As) by the end of fiscal year 2006. Related to these actions, DHS has implemented a Department POA&M [Plan of Action and Milestones] process and an enterprise system to manage the DHS POA&M. Evidence that DHS is successfully institutionalizing the POA&M process is demonstrated by the fact that our initial FY03 POA&M contained less that 100 line items while our current POA&M contains several thousand line items.

Furthermore, DHS has implemented a Certification and Accreditation or C&A tool that will ensure C&A quality and map the C&A testing to the DHS policy. The C&A remediation plan will include a prioritized list of systems to be certified based on the system's security impact level (i.e., systems with high security impact levels will be the first systems to be accredited). The C&A remediation plan will identify a variety of funding alternatives for completing the C&As, our new automated security management tools are already designed to streamline the process. Use of this tool has been mandated for all C&A activity initiated after April 10.

This aggressive remediation effort will provide a sound baseline of secure systems with appropriate controls in place; however, we must continue to improve our security posture throughout the lifecycle of each and every system or application in use in the Department. For this reason, we are continuing to refine the Program so that it will remain relevant for the future. Program enhancements currently underway include:

- Developing a Communications Plan for the DHS Information Security Program, to include an Information Security Portal that will improve the availability of information security data to DHS employees who do not have access to DHS Online.

- Publishing an updated Information Security Program Strategic Plan outlining a revised vision for the future of the program based on lessons learned over the past two years.

Finally, to sustain a viable and healthy Information Security Program, I know that we must have strong support throughout the Department. Through the DHS Chief Information Officers' Council, I will work with each member to ensure that we not only continue to improve our security posture through periodic Program reviews, but that we also implement new and improved measures wherever appropriate. Thank you and I look forward to your questions.

Chairman TOM DAVIS. Thank you very much.

Mr. Alves.

STATEMENT OF TED ALVES

Mr. ALVES. Thank you. Thank you, Mr. Chairman, and members of the committee for the opportunity to testify on the progress the Department of Transportation has made and the challenges it faces implementing FISMA.

This committee has been a driving force behind improvements made over the last several years in protecting Federal information and information systems. I also want to take this opportunity to compliment OMB, NIST, and GAO for the leadership roles they have played in this effort.

With an annual IT budget of about $2.7 billion, the Transportation Department maintains over 480 systems to carry out the Department's mission. For example, the Department operates financial systems that process over $35 billion in grants to States and local governments, and the Federal Aviation Administration relies on about 100 systems to provide safe and efficient air traffic control 24 hours a day.

As you requested, I will discuss the progress Transportation has made and the challenges it faces to strengthen information security practices, the need for a framework to guide Inspector General FISMA audits, and the approach we take to audit computer security issues.

The commitment to improve information security begins at the top, and we attribute much of the Department's progress over the last 2 years to the support provided by Secretary Mineta. In early 2003, the Secretary appointed a Chief Information Officer and significantly strengthened his roles and responsibilities. Since then, the CIO has played a much more prominent role in managing IT issues in all DOT component agencies.

Key improvements the Department has made include the following four areas. First, the CIO invigorated the Investment Review Board, which now considers security issues when reviewing the major systems.

Second, the Department enhanced its ability to protect systems from internal and external attacks by, among other things, establishing an incident response center to prevent, detect, and analyze intrusions from the Internet.

Third, the Department increased the number of certified and accredited systems from 33 percent to over 90 percent by dedicating resources to do the reviews and by closely monitoring progress.

And fourth, the Department significantly strengthened background checks on contractor personnel.

Notwithstanding this progress, DOT still faces challenges to secure its systems. These include: The Department needs to enhance security over air traffic control systems. We have reported that security deficiencies affect en route computer systems which control high altitude traffic. Because the issues are sensitive, we can only cover two issues today.

First, FAA certified that en route systems were secure, but the review was limited to a developmental system. FAA has agreed to review operational systems deployed at the 20 en route centers.

Second, FAA agreed to identify a contingency plan to restore air service in the event of a prolonged en route center disruption.

We recently expressed concern about FAA's progress correcting these deficiencies to the FAA Administrator, the Office of the Secretary, and the CIO, and we are working closely with those officials to ensure continued progress.

The Department needs to improve the security certification process. We also found some deficiencies in the quality of certification reviews, including inadequate risk assessments, lack of evidence that tests had been performed, and in one case a test item failed when we retested it. The Department also needs to continue its focus on emerging threats.

The fact that you raised the question of whether a framework is needed to help standardize IG FISMA reports suggests that the current framework does not fully meet oversight requirements. This issue is being addressed by the President's Council on Integrity and Efficiency, a group of Presidentially appointed IGs, but they have not yet reached a consensus. We think a broader discussion involving the key players, congressional staff, OMB, GAO, and the IG community could help forge a consensus among all interested parties. The IG community would benefit from better understanding how our FISMA reports are used by oversight organizations; oversight organizations would benefit from understanding the challenges the IG community faces addressing computer security issues at agencies with very different system risks and missions.

Regarding our approach to meet FISMA requirements, each year we do detailed tests on a subset of systems to answer OMB's specific questions such as the number of systems with contingency plans. We also perform computer security audits focused on specific systems of security issues. We use all of this work to reach conclusions about the status of DOT's Information Security Program when preparing our annual FISMA report.

Mr. Chairman, this concludes my oral testimony. I would be happy to answer any questions.

[The prepared statement of Mr. Alves follows:]

Before the Committee on Government Reform
U.S. House of Representatives

For Release on Delivery
expected at
10:00 a.m. EST
Thursday
April 7, 2005
CC-2005-025

Department of Transportation's Implementation of the Federal Information Security Management Act

Statement of Theodore Alves
Assistant Inspector General for Financial
And Information Technology Audits
U.S. Department of Transportation

Mr. Chairman, Ranking Member Waxman, and Members of the Committee:

Thank you for the opportunity to testify today on progress and challenges the Department of Transportation (DOT) faces in implementing the Federal Information Security Management Act (FISMA). This Committee has been a driving force behind the improvements the Federal Government has made in protecting important information and information systems over the last several years. These improvements are essential to prevent the severe disruptions that can result from attacks by hackers or by others who are intent on harming the United States and its citizens. I also want to take this opportunity to compliment the Office of Management and Budget (OMB), the National Institute for Standards and Technology (NIST) and the Government Accountability Office (GAO) for the leadership roles they have played in this effort.

The Department of Transportation's 12 component agencies are responsible for one of the largest information technology (IT) investment portfolios among civilian agencies. An annual budget of about $2.7 billion supports over 480 information systems that are critical to carrying out the Department's mission of ensuring fast, safe, efficient, accessible, and convenient transportation. For example, the National Highway Traffic Safety Administration maintains a safety defects information system that receives manufacturer early warning reporting information to track and manage automobile defect and recall data. The Federal Highway and Federal Transit Administrations maintain systems that process over $35 billion in grants awarded to states and local governments.

The Federal Aviation Administration (FAA) operates about 100 systems to provide safe and efficient air traffic control services. Recognizing the critical role the air traffic control system plays in the nation's economic health and the mobility of our citizens, the President determined that the air traffic control system is a critical national infrastructure that must be protected from attack and must be able to reconstitute its operations rapidly in the event of an attack.

The results of fiscal year (FY) 2004 FISMA reports provided by Federal agencies and the Offices of the Inspectors General (OIG) show that a number of agencies have made significant progress meeting the goals set out by this Committee and OMB. DOT is one of the agencies that made significant progress last year and should be proud of the progress it has made. It is also important to recognize that Federal agencies, including DOT, are in the early stages of protecting their information and information systems and that continued attention must be paid to strengthening security to protect against evolving threats. Understanding the actions DOT has taken to improve its security posture may help the Committee to identify actions needed at other departments that have made less progress.

You asked us to address DOT's progress in strengthening information security practices and the challenges it still faces, whether the Inspector General (IG) community needs an auditing framework to guide computer security audits, and the approach we take to audit computer security issues in DOT. Today I will discuss each of those issues.

DOT Made Significant Progress Improving Information Security

DOT made significant progress over the last 2 years protecting its information and information systems, but still faces challenges to secure its systems. To a large extent, DOT's progress can be directly attributed to the support and commitment of Secretary Mineta.

This progress was accomplished against a backdrop of increased attention to this important issue. In addition to the annual FISMA audit, DOT's efforts to enhance its information security program are closely monitored by OMB as part of the President's Management Agenda. The President also issued several directives requiring agencies to protect the Nation's critical infrastructure.

The commitment to improve information security begins at the top, and we attribute much of the improvement DOT has made in this area to support from Secretary Mineta. In early 2003, the Secretary appointed a Chief Information Officer (CIO) and significantly strengthened his role and responsibilities. Since then, the CIO has played a much more prominent role in managing IT issues, including ensuring that the Department adopted disciplined processes to enhance its information security program in all DOT component agencies.

The following summarizes major improvements made by the Department.

- **Increased focus on security in IT investment decisions.** DOT is currently consolidating its Headquarters IT infrastructure by combining the services currently provided by 11 component agencies into a single infrastructure. In addition to reducing costs and improving operations, reducing the number of system access points and the number of potential vulnerabilities should significantly improve security.

- **Strengthened DOT's ability to protect networks from internal and external attacks.** In 2003, DOT established a Department-wide security incident response center. This center, which operates 24 hours a day, prevents, detects, and analyzes hundreds of potential intrusions from the Internet. During FY 2004, DOT expanded its vulnerability checks to cover not only its public web sites but also computers on internal networks. DOT's recent

progress contrasts sharply with its prior efforts to protect its systems. In 1997, we reported that the Department lacked firewalls to prevent outsiders from accessing sensitive internal systems from the Internet. In 2000, we reported that the Department had installed firewall security; however, it was not properly managed. As a result, our staff was able to penetrate the firewall and gained unauthorized access to 250 DOT computers from the Internet. Today, DOT not only has strengthened security over the Internet entry points (the "front door") but also other network connection points (the "back door") to DOT systems.

- **Increasing the number of systems certified and accredited from 33 percent to over 90 percent.** System security certifications are a critical and effective way to provide confidence that systems are secured commensurate with their individual operational risks. DOT trailed behind the Government average by having only 10, 12, and 33 percent of its systems completing such reviews during FYs 2001, 2002, and 2003, respectively. During FY 2004, DOT made a concerted effort to increase the number of system security certification reviews by dedicating resources to do the reviews and closely monitoring progress.

- **Strengthened background checks.** DOT improved its security practices by performing background checks on contractor personnel hired to perform sensitive work such as administering DOT networks. We previously reported a widespread lack of background checks on contractor personnel. This was a major concern to DOT due to the large number of contractor personnel, estimated to be around 18,000. In recent years, the Department established better mechanisms to track contractor personnel movement and ensured that the background checks were performed regardless of the contract length.

DOT Faces Challenges Improving Information Security

Notwithstanding recent progress, DOT still faces many challenges to secure its computer systems. This will require continued senior management attention to implement more disciplined risk-based computer security processes. Our FY 2004 FISMA report cautioned that DOT, and FAA in particular, needed to follow through aggressively in implementing corrective actions to prevent the security program from deteriorating into a significant deficiency in FY 2005. The following summarizes key challenges facing the Department.

- **Air traffic control system security must be enhanced.** We have reported several significant security deficiencies affecting air traffic control en route computer systems, which are used to support high-altitude traffic. Because of the sensitive nature of these deficiencies, we can only discuss two of the issues at this public hearing. First, although FAA had certified that the en route

systems were adequately secured, the reviews were limited to developmental systems located at FAA's Technical Center computer laboratory. Operational systems deployed to the 20 en route centers also need to be reviewed because they are not mirror images of the developmental systems. Second, FAA has agreed to identify a cost-effective contingency plan to restore essential air service in the event of a prolonged en route center service disruption.

We recently communicated to the FAA Administrator, the Office of the Secretary, and the CIO our concern that FAA has not made sufficient progress correcting these deficiencies. We are working closely with the departmental and FAA CIOs to ensure continued progress. FAA needs to continue to make progress to prevent the security program from deteriorating into a significant deficiency in FY 2005.

- **Security certification process needs to be improved.** The Department made good progress in completing these reviews during FY 2004. However, our review of the quality of the certification reviews identified various deficiencies, such as inadequate assessments of the risks facing the system; lack of evidence that tests were performed; and in one case, a test item that had been listed as "passed" failed when we re-tested it. We also found that the appropriate senior official did not always make the decision to allow the system to operate. Obtaining system accreditation from the correct authorizing official is critical because this official not only has to accept the system risk (impact) on business operations but also has to have the authority to allocate budget resources to secure the system. The CIO office agreed to continue its efforts to enhance security certification and accreditation reviews.

- **DOT needs to focus attention on emerging threats from new technologies.** Evolving technologies create new vulnerabilities. DOT needs to continually be on guard to understand the emerging risks that come from new products, and new threats as hackers discover new ways to exploit software vulnerabilities. The CIO Office needs to consider emerging threats such as spyware (malicious software used to capture sensitive user information), phishing (emails leading users to compromised websites), or unsecured wireless communications.

Framework for Auditing Information Security Issues

In your invitation to us to testify, you asked us to discuss whether a framework for information security audits is needed. The fact that you raised this question suggests that the current framework does not fully meet oversight requirements. The DOT OIG supports and participates in several efforts to develop better computer security guidance for agencies and auditors to use, including an effort initiated by the President's Council on Integrity and Efficiency—a group of

Presidentially appointed IGs—to develop additional guidance for FISMA reporting. This group has begun looking at whether more standardization is needed but has not reached a consensus.

The IG community would benefit from greater clarity and understanding of how IG FISMA reports could be better structured to benefit both oversight organizations, such as this Committee, and the affected Department. Similarly, oversight organizations would benefit from understanding the challenges the IG community faces in addressing computer security issues in agencies with very different systems and missions. Discussions about this issue could help achieve a consensus. A key near-term action would be for the key players—OMB, GAO, congressional staff, and the IG community—to begin discussions of the pros and cons of increased standardization. Overall, we believe certain aspects of FISMA audits lend themselves to a more structured framework. The IGs also need to have the flexibility to deploy their limited resources in a cost-effective way to address the unique and evolving threats faced by their agencies.

Our Approach To Meet FISMA Requirements

The DOT OIG uses a two-pronged approach to meet the FISMA reporting requirements. Every year, we select a subset of systems and do detailed tests to answer the OMB performance measure questions, such as the percentage of systems with contingency plans tested. Throughout the year, we also perform various computer security audits with a focus on issues critical to DOT's mission. For example, we are currently conducting reviews of a system used by FAA to maintain air traffic control field equipment, a system used by the National Highway Traffic Safety Administration to track problem drivers, and the network infrastructure used by the Federal Railroad Administration to support its safety inspection program. Based on all this work, we then make judgments about the strengths and weaknesses of DOT's information security program when preparing our annual FISMA report.

We primarily rely on our IT audit staff to perform FISMA-related work, with limited contractor help in reviewing financial systems. Our staff consists of auditors, IT specialists, and computer scientists. This skill mix allows us to address both IT management and technical issues. In conducting our work, we follow GAO, NIST, and OMB guidance. Although neither FISMA nor OMB requires that our FISMA report meet Government auditing standards, we prefer to do so.[1] We believe that reports based on Government auditing standards provide users with more assurance that the underlying work can be relied on for decision-making purposes.

[1] FISMA allows IGs to issue either an audit report or an evaluation report. Audit reports must comply with Government auditing standards established by GAO, while evaluation reports do not.

Mr. Chairman, this concludes my oral testimony. More details are provided below. I would be happy to answer any questions.

PROGRESS DOT HAS MADE AND CHALLENGES IT FACES TO IMPROVE INFORMATION SECURITY

The Department has significantly improved its information security program over the last 2 years, and those improvements account for the significant strides DOT made in FY 2004. This progress is the result of strong commitment and support from Secretary Mineta who, in early 2003, significantly strengthened the CIO's role and responsibilities. Before FY 2003, the CIO did not play a central role in ensuring that IT systems were secured against attack. Since then, the CIO's role in Department-wide IT issues, including computer security, has become much more prominent. The CIO, with support from the Secretary and other senior leaders, has made good progress ensuring that component agencies take the steps needed to ensure their systems are secure. For example, the CIO Office now performs oversight of the quality of component agency IT system security reviews. That oversight provides added assurance that systems have been adequately secured.

The attributes of effective Information Resources Management and computer security programs begin with a commitment and support at the top of the organization. The commitment requires the appointment of a strong CIO with the authority and resources to set direction, provide the correct mix of skills to do the job, establish policies and guidelines, and ensure that subordinate organizations implement disciplined practices. When we began focusing resources on computer security issues back in the late 1990s, DOT did not have those attributes. In fact, we found an almost total lack of attention to protecting critical systems and information. To illustrate, in April 1997, we reported that the Department's computer systems lacked firewalls to prevent outsiders from accessing sensitive internal systems and information directly from public pages on the Internet. Over the next several years, we identified additional weaknesses, including unprotected telephone connections to DOT computer systems, a lack of background investigations for staff performing sensitive functions, and the lack of an effective process to certify systems as secure.

While DOT officials worked for several years to address these problems, their efforts were hampered initially by the lack of a strong CIO with the authority and resources to implement disciplined processes or to require the various component agencies to take computer security issues seriously. As a result, in FY 2000, we were still able to gain unauthorized access to 250 DOT computers through the Internet.

In November 2002, the Inspector General testified that the Department lacked those attributes. He pointed out that DOT had a long way to go to secure its computer systems and in fact had operated for the prior 1½ years without a CIO.

He specifically recommended that the Department promptly appoint a CIO with the authority to provide Department-wide leadership and enforce compliance with security guidance. The Inspector General's testimony also occurred against the backdrop of the President's effort to focus attention on computer security issues through the President's Management Agenda and to better protect critical national infrastructures through Presidential Decision Directives. The Department took the following actions:

- Secretary Mineta appointed a CIO in March 2003 and ensured that the CIO had the authority to implement disciplined information resource management and computer security practices;

- Within months, the CIO provided strong leadership by invigorating the Investment Review Board, which reviews IT investments to determine whether they should be modified, terminated, or allowed to continue. The Investment Review Board is headed by the Deputy Secretary with support provided by the CIO Office.

- The CIO has secured a commitment from component agencies to implement the Department's information security program. This effort is being carried out with the help of over 400 trained information security personnel. The CIO and component agencies also supplement these staff with contractor resources to address key technical issues.

- The CIO has made good progress implementing disciplined processes to enhance the information security program. For example, DOT has established a risk-based approach to perform system security reviews and to test system security. DOT also provides specialized training to security specialists.

- The CIO Office also took on more operational responsibilities, including establishing a full-time unit to monitor activity on all DOT networks. This has significantly strengthened DOT's ability to detect and report attempted intrusions into DOT networks.

The CIO's broader responsibilities led to increased funding needs to support the more disciplined processes and more intensive reviews, as well as the new operational responsibilities. However, the CIO Office needs to provide better justification for its IT budget requests. Because of the high level of generality and vagueness in the budget justification, Congress reduced the CIO Office's FY 2004 budget by $15.9 million, from $23.4 million to $7.5 million. Our review confirmed that the CIO's budget request and supporting documentation lacked the details oversight organizations, including OMB and Congress, needed to understand how the funds would be used.

The CIO Office subsequently had to submit to both the House and Senate Committees on Appropriations a reprogramming request of about $2.5 million to cover costs associated with computer security activities, including funding to support its certification and accreditation reviews. The Committees approved the reprogramming, and the CIO Office agreed to provide more complete information in future budget requests, so that decision-makers can make informed decisions about the appropriate level of funding.

The CIO also needs to improve how security-related budget requests are coordinated between the CIO Office and component agencies. For example, in its FY 2005 budget, the CIO Office requested $2 million to install advanced vulnerability remediation and patch management software to protect the Department's IT infrastructure. About 90 percent of the installation would have been on FAA network computers. However, FAA had also set aside funds to acquire a similar solution, and the two requests had not been adequately coordinated.

DOT's Progress Improving Information Security

The changes instituted by Secretary Mineta led to significant improvements in DOT's ability to secure its information and information systems over the last 2 years and especially in FY 2004. Some of the most noteworthy progress DOT has made in information security includes:

- **Increased focus on security in IT investment decisions.** The departmental Investment Review Board expanded its review of component agency investment projects to ensure that investment plans adequately addressed security issues. The CIO also directed component agencies to evaluate opportunities to consolidate common administrative and business systems. For example, DOT is currently consolidating its Headquarters IT infrastructure by combining the services currently provided by 11 component agencies into a single infrastructure. In addition to being an important initiative to reduce costs and improve operations, it should also significantly improve security by reducing the number of system access points and therefore, the number of potential vulnerabilities.

- **Strengthened ability to protect networks from internal and external attacks.** DOT has made significant progress protecting its systems from internal and external attacks. This serious problem persisted for several years. In 2003, DOT established a Department-wide security incident response center. In cooperation with a similar center operated by FAA, this center operates 24 hours a day to prevent, detect, and analyze hundreds of potential intrusions from the Internet. During FY 2004, DOT expanded its vulnerability

checks to cover not only its public web sites but also computers on internal networks in all component agencies. The CIO Office also issued guidelines for configuring computers in a secure manner to prevent vulnerabilities.

- **Increased the number of systems certified and accredited from 33 percent to over 90 percent.** System security certifications are a critical and effective way to provide confidence that systems are secured commensurate with their individual operational risks. This action provides additional assurance that DOT program operations that depend on computer systems support can maintain the integrity, confidentiality, and availability of the information they rely on to carry out their missions.

- **Strengthened background checks.** DOT also made significant progress ensuring that background checks are performed on contractor staff performing sensitive services. Previously, we found that DOT did not require all contractors to undergo background checks and even when the checks were required, many were never performed. DOT improved its security practices by requiring background checks for all contractor personnel performing sensitive activities, regardless of the contract length. Previously, background checks were not performed if the contract term was for less than 6 months.

Challenges to Sustain This Progress

Notwithstanding recent progress, DOT still faces many challenges to secure its computer systems. This will require continued senior management attention to implement more disciplined risk-based computer security practices. This is key to ensuring that critical information and systems are secure, especially the air traffic control system. For example:

- **Air traffic control system security must be enhanced.** During FYs 2003 and 2004, we reported several significant security deficiencies associated with air traffic control en route computer systems. En route systems control high-altitude traffic. Because of the sensitive nature of these deficiencies, we can only discuss two of the issues at this public hearing. We have previously discussed all of the issues with this Committee's staff.

  First, although FAA certified that the en route systems were adequately secured, the reviews were limited to developmental systems located at FAA's Technical Center computer laboratory. Operational systems deployed to en route centers also need to be reviewed. FAA has agreed to review operational en route systems by the end of FY 2005 and to review all other air traffic control systems—at approach control and airport terminal facilities—by the end of December 2007.

Second, FAA has agreed to identify a cost-effective contingency to restore essential air service in the event of a prolonged service disruption at an en route center. This is important because the President has designated the air traffic control system to be a critical national infrastructure. Presidential guidance calls for critical infrastructures to have contingency plans in place to restore essential services in a timely manner. FAA will use the results of an alternatives analysis to identify cost-effective alternatives. FAA needs to focus now on the near-term actions it can take to restore partial services in the event of a prolonged disruption.

- **The security certification process needs to be improved.** The security certification review, which is performed by system owners in conjunction with the CIO Office, is a critical and effective security measure to determine whether individual systems are adequately secured commensurate with operational risks. The Department made good progress in completing these reviews during FY 2004. However, the CIO office needs to continue working with component agencies to improve the quality of the reviews. Our review of the quality of the certification reviews for 20 systems identified 1 or more deficiencies in 14 cases. These deficiencies included inadequate assessments of the risks facing the system; lack of evidence that tests were performed; and, in one case, a test item that had been listed as "passed" failed when we re-tested it.

  We also found that the appropriate senior official did not always make the decision to allow the system to operate. One of the most important steps in completing a security certification and accreditation review is the responsible senior official's (the system user's) decision whether to accept the remaining security weaknesses and allow (accredit) the system to operate. Obtaining system accreditation from the correct authorizing official is critical because this official not only has to accept the system risk on business operations but also has to have the authority to allocate budget resources to secure the system. In 4 of 20 systems we reviewed, technical managers and not the appropriate senior official accredited the systems for operations. The CIO office agreed to continue its efforts to enhance the process of the security certification and accreditation reviews.

- **DOT needs to focus attention on emerging threats from new technologies.** Evolving technologies create new vulnerabilities. DOT needs to continually be on guard to understand the emerging risks that come from new products and new threats as hackers discover new ways to exploit software vulnerabilities. The CIO Office needs to consider emerging threats associated with technologies, including:

- Software, called spyware, that allows malicious individuals to covertly capture sensitive information from a user's system,

- Phishing, which is a form of email that directs users to a compromised web site that then solicits personal, financial, or business information.

- Wireless technologies, which can increase risks that agency information will be compromised. Wireless technology poses a threat in part because the devices tend to be managed by individuals, who may be less security conscious than system administrators.

Overall Security Program Status

Our FY 2004 FISMA report concluded that based on the progress the Department made, the overall status of the security program, and FAA's commitment to take aggressive action to correct air traffic control deficiencies, DOT's information security program warranted downgrading from a material weakness to a reportable condition. We cautioned, however, that DOT, and FAA in particular, needed to followed through aggressively in implementing corrective actions to prevent the security program from deteriorating into a significant deficiency in FY 2005. We cited FAA's progress reviewing operational systems and implementing en route center contingency plans as a key factor we will use in making our determination of whether DOT's security program contains significant deficiencies in FY 2005.

Now, 6 months later, we are concerned that FAA has not made sufficient progress correcting en route air traffic control deficiencies we reported last year, including security certification reviews of computer systems at en route centers and development of contingency plans to restore air traffic control services in case of a prolonged service disruption at an en route center. We have communicated these concerns in writing to the responsible DOT officials, including the CIO, the Office of the Secretary, and the Federal Aviation Administrator. The FAA CIO responded to those concerns, indicating FAA's continued commitment to pursue timely implementation of corrective actions. We are now engaged in further discussions with the departmental and the FAA CIOs about the actions needed to ensure continued progress to address these important issues.

FRAMEWORK FOR AUDITING INFORMATION SECURITY

The fact that you raise the question about whether a framework for information security audits is needed indicates that the current framework does not fully meet your oversight requirements. The DOT OIG supports and participates in several efforts to develop better computer security guidance for agencies and auditors to

use,[2] including an effort initiated by the President's Council on Integrity and Efficiency—a group of Presidential appointed IGs—to develop additional guidance for auditing security issues and for reporting FISMA results. This group has begun looking at whether more standardization for FISMA reporting is needed but has not reached a consensus.

The IG community would benefit from greater clarity and understanding of how IG FISMA reports could be better structured to benefit both oversight organizations, such as this Committee, and the affected Department. Similarly, oversight organizations would benefit from understanding the challenges the IG community faces in addressing computer security issues in agencies with very different systems and missions. Discussions about this issue could help achieve a consensus. A key near-term action would be for the key players—OMB, GAO, congressional staff, and the IG community—to begin discussions of the pros and cons of increased standardization. Overall, we believe certain aspects of FISMA audits lend themselves to a more structured framework. The IGs also need to have the flexibility to deploy their limited resources in a cost-effective way to address the unique and evolving threats faced by their agencies.

Some key issues that the DOT OIG believes need to be considered in this dialogue follow.

- **The IG community needs to retain the flexibility to address the unique and evolving threats and vulnerabilities faced by each agency.** Both agencies and auditors need the flexibility to focus their resources on the burning issues of the day. We all need to use a risk-based approach to strengthen computer security, and we need to adjust our focus to address evolving risks. For example, DOT maintains a wide variety of systems with very different vulnerabilities and consequences. The consequences from an attack on a system that maintains information about employee training are very different than the consequences of an attack on an air traffic control system. Similarly, because agencies have achieved different levels of maturity in addressing computer security issues, agencies and auditors must focus their limited resources on the most vulnerable security processes faced by the agency. For example, some OIGs are still reporting that their agencies lack a complete inventory of systems or a reliable system to track vulnerabilities and action plans. Those agencies and their auditors need to be

[2] Our Deputy Assistant Inspector General for Information Technology and Computer Security is also a member of the Information Security and Privacy Advisory Board. The Board is responsible for advising NIST and the OMB Director on information security and privacy issues pertaining to Federal Government information systems. The Board was established by the Computer Security Act of 1987 and reauthorized by FISMA.

able to focus their attention on getting those basic processes in place to correct those high-risk deficiencies.

- **NIST and GAO have provided a common framework for implementing and auditing computer security.** NIST recently issued a series of guidelines and standards for agencies to use, as required by FISMA. We find NIST guidance to be very useful because it is generally complete, adequately detailed, and authoritative. DOT applies NIST guidance, and we use it as criteria when we evaluate how effectively DOT's security program is operating. GAO has also issued guidance for auditing security over individual computer systems, called the Federal Information Systems Control Audit Manual. The entire IG community commonly uses this manual when auditing security over individual systems.

- **Agencies and auditors also need to ensure that they devote adequate resources to improve all information resources management processes.** This is because computer security is an important subset of information resources management. Instituting disciplined management practices is critically important to ensure that agencies receive value for the billions of dollars spent on IT, but it is also critical to ensure adequate security. Efforts to strengthen the CIO and Investment Review Board functions have spill-over effects that lead to improved computer security. For example, a strong investment review process can build computer security into the system, a much more cost-effective approach than identifying and correcting deficiencies after system deployment. Some estimates show it costs 10 times as much to correct problems after deployment.

- **Financial statement and FISMA audits**. You also asked whether financial statement audit guidance provides a model for computer security audits. The American Institute of Certified Public Accountants developed the financial statement audit requirements, which are supplemented by the GAO's Financial Audit Manual. Financial audit guidance has evolved continuously over the last 100 years, most recently to incorporate the stronger requirements to audit management controls imposed by the Sarbanes-Oxley Act. Most IGs also conduct a wide range of other financially related audits to address financial management issues that are not covered by financial statement audits. Because computer security did not receive a lot of attention until about 20 years ago when Congress passed the Computer Security Act of 1987, information security audits are still in their infancy. Certain aspects of information security audits clearly lend themselves to a structured framework, including network vulnerability assessments, system penetration testing, and intrusion detection and incident response capabilities.

OUR APPROACH TO MEETING FISMA REQUIREMENTS

The DOT OIG approaches the FISMA reporting requirement as a part of our efforts to ensure that DOT has effective IRM processes in place. We perform a series of computer security audits during the year focused on the issues we believe involve the highest risk or the issues that most need management's attention. The results of those efforts are then included in our annual FISMA report.

Throughout the year, we focus a significant amount of our IT resources on information security issues. Our IT audit staff consists of auditors, IT specialists, and computer scientists. This mix of IT management and technical skills allows us to address both the management processes and the detailed technical issues the Department faces as it strengthens its computer security capabilities. For example, we use our computer scientists to do very technical reviews, including penetration testing or identification of system design or software flaws. We use our IT auditors to analyze the quality of management processes, like the certification and accreditation process, and to make constructive recommendations to strengthen processes. As we stated earlier, disciplined processes are essential to an effective computer security program. We also hire contractors to help us audit computer controls related to financial systems.

To be ready to meet the annual FISMA reporting requirement, we monitor the CIO's efforts to comply with OMB reporting requirements throughout the year. After OMB issues its guidance specifying which performance measures it wants tracked, we select a subset of systems and do detailed tests of the source data to answer the OMB performance measure questions. Our FISMA report also draws on all other audit work we have done during the year to make judgments about the strengths and weaknesses of DOT's computer security efforts.

For example, we recently initiated two computer security audits. We are reviewing the National Highway Traffic Safety Administration's National Driver Registry system. The system is a central repository of information about individuals who have had their driver's license suspended or revoked. The information that resides on the system, such as social security numbers, is subject to Privacy Act protection. Unauthorized disclosure of this information could lead to identity theft, a problem that has affected nearly 10 million Americans. We will review this system to ensure that the information is reliable and that access to the information is only available to authorized personnel. We have discussed this audit with your staff members who have expressed interest in the results.

We are also reviewing the Federal Railroad Administration's (FRA) network infrastructure, which is critical to the missions of DOT and FRA. FRA is one of five DOT component agencies that have its own direct Internet connections,

allowing the public to access the DOT network from the Internet. We will review the network infrastructure to ensure security weaknesses do not exist that could jeopardize the confidentiality, integrity, and availability of the data residing on FRA and DOT systems.

In conducting our work, we follow GAO, NIST, and OMB guidance. GAO establishes Government auditing standards, which we follow in performing computer security audits. Although neither FISMA nor OMB requires that our FISMA report meet Government auditing standards, we prefer to do so. We believe that reports based on Government auditing standards provide users with more assurance that the underlying work can be relied on for decision-making purposes.

Chairman TOM DAVIS. Thank you very much.

Mr. Matthews, last but not least here.

STATEMENT OF DANIEL MATTHEWS

Mr. MATTHEWS. Thank you, Mr. Chairman, and members of the committee. I thank you for the opportunity to appear here today to discuss the Department of Transportation's implementation of the Federal Information Security Management Act of 2002 [FISMA].

I serve as the Department's CIO, and I also currently serve as the vice chair of the CIO Council. The DOT Office of the Chief Information Officer has operational responsibility for the departmental network and communications infrastructure as well as providing shared services for the Office of the Secretary and the operating administrations currently engaged in the Department's information technology services consolidation.

FISMA compliance at DOT is moving from the intensity of the past year's implementation activities to a more operational mode. Our system inventory is mature, our certification and accreditation methodology is defined, and we have begun oversight of the remediation of weaknesses identified over the course of the last 2 years. Additionally, we have been in the process of making assessments of the Department's ongoing security posture. Securing the IT assets of the Department of Transportation is a critical responsibility that falls to the CIO's office.

In striving to secure those assets, many people from various areas must pull together. The strides the Department has made over the past year occurred in large measure because of the support of Secretary Norman Y. Mineta. His leadership and guidance combined with each and every modal administrator's commitment are critical to the Department's success.

We are pleased to have achieved an A-minus rating on the FISMA scorecard, and we note that DOT relied on teamwork across the agency, the establishment, refinement, and validation of our system inventory, good communications, comprehensive training, and the support of the Inspector General throughout the year. This last point is critical. With our Inspector General, who is engaged, involved, and informed throughout the process, DOT makes sure that it approaches FISMA requirements appropriately and the end products and results are supportable.

The teamwork for FISMA compliance was established through the acceptance of a single departmentwide methodology in lieu of individual approaches established by each operating administration. That methodology allowed us to focus and work collectively on a single plan in which all participants had confidence. This gave us the benefit of synergy, an end greater than the sum of its individual parts.

If we endeavor to proceed using agency unique approaches, some agencies may have been successful and some may have faltered. With the support of an industry-recognized security subject matter expert from Titan Corp., along with agencywide buy-in and acceptance, DOT was able to reduce overall certification and accreditation schedules, manpower requirements and costs. More importantly, DOT was able to ensure accuracy, consistency, and completeness of each accreditation package.

The strides made over the last year to comply with FISMA requirements were impressive. DOT has accredited over 90 percent of all operational IT systems, established a program to ensure security as part of every system's development life cycle, significantly reduced vulnerabilities of public facing systems, and improved training and communications at all levels of the organization.

Moving forward, DOT is using metrics to gauge FISMA's implementation and compliance throughout the Department. This point is important. DOT recognizes that plans of actions and milestones, POA&Ms, are established from the certification and accreditation process required by FISMA and are reviewed by the Inspector General. DOT uses these POA&Ms as a mechanism to ensure we mitigate the risks and remediate vulnerabilities identified during the CNA process knowing full well that the actions taken prescribed in the POA&M will specifically improve DOT's overall security posture.

To address the steps DOT is taking to further strengthen IT security, we are coordinating and cooperating with DHS on cyber exercises, we are addressing the critical need for enterprise-wide vulnerability management, we are implementing baseline security configuration standards for critical software, and we are consolidating IT services.

More needs to be done. The FAA's National Air Space System is part of the national critical infrastructure program. I am working directly with the FAA senior leadership and the Inspector General to ensure FAA secures and protects the important NAS systems and telecommunications infrastructure. Ensuring the FAA constructs are measurable plans of actions in conjunction with its POA&Ms, audit reports, and IG findings, with follow through to complete its commitments is fundamental to DOT's ability to maintain current FISMA scorecard ratings.

I have included in my statement some specific observations and suggestions for creation of an "as of date" and believe that existing FISMA guidance is adequate but have some additional comments. I look forward to answering your questions. And, again, I thank you for this opportunity.

[The prepared statement of Mr. Matthews follows:]

U.S. DEPARTMENT OF TRANSPORTATION
CHIEF INFORMATION OFFICER TESTIMONY
BEFORE THE
HOUSE COMMITTEE ON GOVERNMENT REFORM

Mr. Chairman and members of the Committee, thank you for the opportunity to appear today to discuss the Department of Transportation's implementation of the Federal Information Security Management Act of 2002 (FISMA).

I serve as the Department's Chief Information Officer (CIO), and I also currently serve as the vice-chair of the Federal CIO Council.

The DOT Office of the Chief Information Officer (OCIO) has operational responsibility for Departmental network and communications infrastructure, as well as providing shared services for the Office of the Secretary and the Operating Administrations (OAs) currently engaged in the Department's Information Technology (IT) services consolidation.

FISMA compliance at DOT is moving from the intensity of the past year's implementation activities to a more operational mode. Our system inventory is mature, our certification and accreditation methodology is defined and we have begun oversight of the remediation of weaknesses identified over the course of the last two years. Additionally, we have been in the process of making assessments of the Department's on-going security posture.

Securing the IT assets of the Department of Transportation is a critical responsibility that falls to the CIO's office. In striving to secure those assets, many people from various areas must pull together. The strides the Department has made over the past year occurred in large measure because of the support of Secretary Norman Y. Mineta. His leadership and guidance combined with each and every modal administrator's commitment are critical to the success of the Department's efforts.

We are pleased to have achieved an A- rating on the FISMA Scorecard and note that DOT relied on teamwork across the agency; the establishment, refinement and validation of our system inventory, good communications, comprehensive training, and the support of the Inspector General throughout the year. This last point is critical. With our Inspector General who is engaged, involved and informed throughout the process, DOT makes sure that it approaches FISMA requirements appropriately and the end products and results are supportable. The teamwork for FISMA compliance was established through the acceptance of a single, department-wide methodology in lieu of individual approaches established by each operating administration. That methodology allowed us to focus and work collectively on a single plan in which all participants had confidence. This gave us the benefit of synergy, and an end greater than the sum of its parts. If we endeavored to proceed using Agency unique approaches some agencies may have been successful, some may have faltered. With the support of an industry recognized security subject matter expert from Titan Corporation, along with agency-wide buy-in and acceptance, DOT was able to reduce overall certification and accreditation schedules, manpower requirements,

and costs. More importantly, DOT was able to ensure accuracy, consistency and completeness of each accreditation package.

The strides made over the last year to comply with FISMA requirements were impressive. DOT has accredited over 90% of all operational IT systems; established a program to ensure security is part of every system's development life-cycle; significantly reduced vulnerabilities of public facing systems, and improved training and communications at all levels of the organization.

Moving forward DOT is using metrics to gauge FISMA implementation and compliance throughout the Department. This point is important. DOT recognizes that Plans of Action and Milestones (POA&Ms) are established from the certification and accreditation process required by FISMA and are reviewed by the Inspector General. DOT uses these POA&Ms as a mechanism to ensure we mitigate the risks and remediate vulnerabilities identified during the C&A process, knowing full well that taking the action prescribed in the POA&M specifically will improve DOT's overall security posture.

To address the steps DOT is taking to further strengthen IT Security:

- DOT is coordinating and cooperating with the Department of Homeland Security on cyber exercises, reporting requirements, and critical new initiatives. One of these initiatives is the IT Security Line of Business. DOT is actively involved with the planning, design, and implementation of this effort.

- DOT is addressing the critical need of enterprise-wide vulnerability management. We are implementing a Department-wide vulnerability remediation program, in part to support an established quarterly compliance review process. The compliance reviews are used to ensure operating administrations are complying with FISMA and other important laws, such as the Privacy Act of 1974.
- DOT is implementing baseline security configuration standards for critical software.
- DOT is consolidating its IT services. This initiative is an important mechanism to secure DOT IT assets and infrastructure. Each operating administration having separately maintained networks across the Department requires multiple applications of patches. If one of those networks is vulnerable, then DOT as a whole is vulnerable. Through consolidation of networks DOT not only significantly improves network security but we gain the added advantage of avoiding redundant costs. Another significant benefit of the consolidation effort is a more complete view of the entire enterprise by the network operations center and the Department's Cyber Incident Response function. Taking this thought one step further, DOT is in a better position to report to, work with, and respond to the Department of Homeland Security, especially when most needed.

More needs to be done. The FAA's National Airspace System is part of the National Critical Infrastructure Program. I am working directly with FAA senior leadership and the Inspector General to ensure FAA secures and protects the important NAS systems and telecommunication infrastructure. Ensuring the FAA constructs measurable plans of actions in conjunction

with its POA&M's, audit reports, and IG findings, with follow-through to complete its commitments, is fundamental to DOT's ability to maintain its current FISMA scorecard rating.

Finally, the Committee asks what additional guidance, procedures or resources are needed by the agencies to improve their information security and fully comply with FISMA?

DOT offers the following observations and suggestions:

- DOT supports the creation of an "as of date" for the annual FISMA Report to OMB. This date would be similar to the fiscal year-end date used in preparing financial reports. The benefits of adopting an "as of date" by federal agencies and IGs, is it would create a "common point" in time for measuring the status of an agency's IT security program, e.g., systems inventory and self-assessments. This "as of date" would eliminate timing differences between an agency's report and the IG report which may be infused by time issues.
- DOT believes existing FISMA guidance published by OMB and National Institute for Standards and Technology is adequate, but at the same time As the Vice Chair of the CIO Council, I am working towards having an annual government-wide FISMA kick-off meeting between Federal CIO Council and the President's Council on Integrity and Efficiency to ensure everyone consistently interprets and applies the guidance and the auditing standards.

In conclusion, it is my observation and experience at DOT that the Department's cyber security initiatives are working well and support DOT's ability to safely and securely deliver critical services to our customers.

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

Chairman TOM DAVIS. Thank you very much.

I think a recurrent theme both with DOT and USAID is that you are getting support at the top, that this comes—it is not just generated from the CO, it is top down, it is holding people accountable. Great stories. I hope we can learn from that.

Mr. Cooper, let me start with you because your department is great but it is down. I don't hold you accountable. You are one of the best CIOs in the business, and we are sorry to see you going. But I wonder if we could talk about, you also, as you could see from some of the early comments from our members, the area everybody wants to focus on. Homeland security is a hot topic. It is an area where the systems need to be up. It is a very difficult job given the type of systems you inherited when we merged the departments. I think we can—that is a given; this was a very, very, very tough job. But we are a long way from where we need to be. We are seeing improvement, and I appreciate your opening statement.

What are the major obstacles you would put together that Homeland Security faces uniquely versus some of the other agencies that make it so difficult?

Mr. COOPER. OK. Let me try to answer that question directly, very specifically and very candidly.

Chairman TOM DAVIS. This is the last bite I get at you.

Mr. COOPER. No, that is all right. I am happy to come back. And let me also try to put it within the context of the FISMA scorecard, because I think this will be extremely helpful, I hope, to the committee as well as to members of the audience and interested parties and my colleagues.

The first thing that we face as the Department of Homeland Security is the fact that we have inherited a huge amount from our legacy environments. Now, that translates to the inventory in the FISMA scorecard. This is not a defense. We are not where we need to be. But the scoring in the scorecard, we get minus 10 points against our total score until we can actually certify that we have inventoried 95 percent of the systems and applications that are in the Department. And here's what we're learning and here's what we found. Meaning no disrespect to my colleagues on the panel, DOT has identified 480, I think Dan said 480 significant applications or the ones that they have identified and accredited. And, again, no offense to AID, but I think you guys have nine. We have over 3,600.

So there's a simple fact, it's a numbers game. All right? We move from 34 percent of that initial 3,600 to 68 percent. Now, the scorecard doesn't reflect the progress. 68 percent I admit is still a failing grade. But we know what we need to do, we are working with our IG, we have demonstrated that our certification and accreditation process is sound. We need to stay the course and apply it. We have committed to completing 100 percent certification and accreditation by fiscal year 2006.

Another major area. Configuration management addresses the different parts and pieces in the FISMA scorecard. Now, what that translates to is how many different operating systems or platforms or environments does the Department have? We have everything that's listed in the scorecard. But I—and I am the one that can be held accountable. I made a tactical and conscious decision that we

were not going to put significant effort into the configuration management aspect of all of the listed platforms for the following reason: We are also undergoing a major IT infrastructure transformation program. We are consolidating those operating platforms and the operating systems and the associated applications, and we are eliminating some of those. Therefore, I made a decision that said don't put any energy into publishing guidelines within the Department in our Information Security Program around configuration management for those platforms and operating systems that we are going to retire. I am the person, I am accountable. But it reflects in our score because we then don't—we legitimately don't have anything in that area.

Another thing, final thing we did very quickly. The training of all DHS employees in information assurance and information security management is an extremely high value activity. It scores very few points on the scorecard. But we consciously made a decision, again. We have trained almost 100 percent of all of our employees across the Department. That's 180,000 people, and we accomplished that in the past 2 fiscal years.

So those are very specific examples in the framework of the scorecard that I think help reveal some of the complexities that we're facing but also significant progress.

Chairman TOM DAVIS. What are the most difficult parts of all the disparate systems that you have? You know, what are the most dysfunctional or most vulnerable areas that you have at DHS?

Mr. COOPER. That's a tough question in that I'm not sure I want to put any parts of the Department on the spot.

Chairman TOM DAVIS. Well, but you inherited legacy systems and some of these. Like we know, the old INS system just wasn't working. Now, we've got new—I mean, this is something that this committee has talked about and everything else. I am not trying to go out to tell terrorists where we are vulnerable or something. But within those confines you have some old legacy systems that you haven't been able to move forward on as quickly as others and stuff like that. Give me a priority list, in other words.

Mr. COOPER. OK. I'm going to share at least the part that we've identified.

Chairman TOM DAVIS. You're leaving now. I can't do anything.

Mr. COOPER. That's true.

Chairman TOM DAVIS. You are under oath, too.

Mr. COOPER. They can fire me early, I guess.

Chairman TOM DAVIS. But we will hire you. We will pick you up if you need it.

Mr. COOPER. Here's what we found. And, again, please understand, I offer this in a very constructive way. It's not meant to be critical.

Chairman TOM DAVIS. Absolutely.

Mr. COOPER. One of the areas that we have found a little bit more challenged is in some of the legacy INS, Immigration and Naturalization Services, and Citizenship and Immigration Services, as those two entities exist now. But in fact those were more or less, I won't say truly combined, but they were all under the auspices of an organizational structure inside the Department of Justice that pretty much operated from the same or similar platforms.

Now, we have broken them apart, so to speak. But in breaking them apart, we actually don't have all of the IT infrastructure and skills and personnel and everything fully in place yet.

Now, again, plans are in place, we are making good progress, but it remains a challenge because we just don't have quite enough of the resources in the timeframe we would like to have to finish a lot of the certification and accreditation, some of the securing activities that we need to do.

Our Customs and Border Protection environment has actually made very, very good progress in a lot of areas, and what we are doing is drawing upon the positive skills and the positive performance in CBP to now reach over and assist ICE and CIS. So we figured out ways that we can actually leverage where we have good stuff going on and address some of the challenge areas.

Chairman TOM DAVIS. How many incidents—well, we don't really get the level of incident reporting. Am I right? We don't get the incident reporting that we'd like to get that we feel is accurate. Is that fair?

Mr. WILSHUSEN. Well, OMB reported that in their 2004 report on FISMA that they felt that the reporting was sporadic from the different agencies, and they had questions and concerns about that.

Chairman TOM DAVIS. Well, let me just go with each agency and ask the CIO or IG or which office; but start with AID. Are you getting a lot of incidents of penetrations every year, and do you test yourself? Do you hire people who come in and try to penetrate? That was inarticulate, but I think you understand.

Mr. STREUFERT. We're initiating some internal testing, and we're constantly monitoring for intrusions, and I think that the most constructive part of that is that we are tracking precisely those patterns and trying to assess who's at us. So, from an internal purpose, we are doing well.

Chairman TOM DAVIS. Is that reported up the food chain in terms of who we think is going after you?

Mr. STREUFERT. We make every effort that we possibly can, and the comments that we collect internally on this topic are some of the descriptions that come out from elsewhere at varying degrees of descriptions, some general, some specific. And so we think an area of potential improvement is having a matching of a good taxonomy externally against what we are actually seeing, and we think that this will improve over time.

Chairman TOM DAVIS. Let me ask Homeland Security. What are you seeing in that area? I don't want you to give away the store, but——

Mr. COOPER. No. First of all, we see hundreds of thousands of attempts on an annual basis. We actually identified 214 incidents. We reported 100 percent of the 214 both to the IG and up through US-CERT that passes over to OMB.

Chairman TOM DAVIS. Do you have a good idea of who the people are that are trying to get in?

Mr. COOPER. Yes, we do, partly because of the link into the intel environment and everything. So, yes, we do. We believe this is an area and it actually is represented in our scorecard where we are in very good shape.

Chairman TOM DAVIS. And it helps you also target your resources when you know who is coming after you. Doesn't it?

Mr. COOPER. Absolutely.

Chairman TOM DAVIS. And how about Transportation?

Mr. MATTHEWS. Mr. Chairman, last year we had over 3,000 incidents and reported them. We do track individuals, Web sites, IP addresses that are coming toward the Department as well as other information. We routinely——

Chairman TOM DAVIS. One of them gets through and really gets into the system, they could run you amuck. Couldn't they? They could really destroy you?

Mr. MATTHEWS. Absolutely, no doubt, if somebody penetrates the shield, indeed they can run amuck. You know, TOPOFF III is currently going on, and when I'm sitting watching what we're doing in TOPOFF III I'm constantly reminded that if someone did a concerted effort and went after the communications of the Federal Government, its ability to respond could be impacted.

Chairman TOM DAVIS. And it helps. I mean, I think it's reassuring to us to know that at least you have a pretty good idea of who is after you.

Mr. MATTHEWS. Yes.

Chairman TOM DAVIS. And that helps you, doesn't it, in terms of where you spend your resources? It may or may not help your report card, but it helps you in terms of where you spend your resources?

Mr. MATTHEWS. Absolutely 100 percent. We work hand in glove with the IG to do the forensics and pursue and prosecute those individuals as well.

Chairman TOM DAVIS. Mr. Alves, do you agree with that?

Mr. ALVES. Yes, I do. The Department of Transportation has made really significant progress in this area over the last couple of years, and whenever there is an intrusion they let us know immediately. We do some of the penetration testing ourselves.

Chairman TOM DAVIS. Some of them are yours.

Mr. ALVES. To test the system and make sure that it's secure.

Chairman TOM DAVIS. And Mr. Cooper, let me just ask you. The fact that you have an idea in most of these cases, I gather, who is coming, allows you to expend resources in those areas, maybe to the detriment of other areas but at least it allows you to give appropriate prioritization, and that ought to give the committee some assurance that you're on top of it.

Mr. COOPER. Yes, sir. In this case, we do. And in this case, because of the capability within the Department, we work very closely with our Homeland Security Operations Centers, we work very closely with our Intelligence Analysis and Infrastructure Protection Directorate, and actually share. All of the key members of my team are cleared to the highest levels, and so we actually use a lot of the classified information to help us address risks, threats, and vulnerabilities.

Chairman TOM DAVIS. OK. You feel—well, we'll have another conversation later. But thank you again. My 10 minutes is up.

Mr. Ruppersberger.

Mr. RUPPERSBERGER. OK. Mr. Deffer, in your testimony you mentioned that FISMA does not differentiate between routine or mission critical systems.

Mr. DEFFER. Correct.

Mr. RUPPERSBERGER. And you continue to say that the agency might still be at risk if its security, a vast majority of its systems yet is left vulnerable, the most mission critical ones. Can you explain how your department has balanced meeting its FISMA obligations with protecting its most critical systems?

Mr. DEFFER. Well, I think the Department has sort of—they've made an effort to get their systems certified and accredited. I don't know if they've—Mr. Cooper talked about this, trying to get them on a risk based methodology to certify and accredit those systems that are high priority. But the numbers don't tell us which systems that have been certified and accredited are really that important. We don't know whether—has their network been certified and accredited? I don't know. But, you know, their training management system FLETC may have been certified and accredited, and that's a good thing, but it's probably not as important as the network or other critical applications.

Mr. COOPER. If I may kind of clarify. We have made a very conscious and deliberate decision to go after our mission critical systems first. So we are taking a risk-based prioritization approach to what we accredit.

The good news that I can share with the committee is that the 68 percent that are now accredited include almost every one of our major mission critical systems, and we are getting to some that doesn't mean they're not important but lesser impact or risk by not accrediting them right away. That is the approach we're taking.

Mr. RUPPERSBERGER. I would like more, a little bit more about the questions that the chairman asked you, and I was going to ask you more questions but you answered some of them. One of the questions was, when do you expect that the Department of Homeland Security will come up to where they need to be? And you mentioned that your goal was 2006. Do you feel that you are on time for that goal at this point?

Mr. COOPER. Yes, we do.

Mr. RUPPERSBERGER. And what is it, the end of the year, beginning of the year? Where are we?

Mr. COOPER. By the end of fiscal year 2006 we expect to complete almost 100 percent of those items represented by the scorecard. Now, here's what is going to happen though, and we will see whether or not I'm a good prognosticator. Unfortunately, the way that we are going at this and the way that the scoring works in the scorecard, I think what we are going to do is we are going to jump. We may indeed be—I'm hoping we will get to a D in fiscal year 2005. I am being very candid here. Because we lose 10 points off of our total score because of this 95 percent requirement for inventory. And we will not complete 95 percent of our full inventory by the end of fiscal year 2005. We are going to be very, very close, but I am not sure we'll trip it. We are going to basically lose 20 points of our score because of the configuration management approach that I explained to you. If you deduct those 30 points from

the score and we do everything else, that's 70, which puts us at 70 percent, which may creep us into a D.

What I think is going to happen is we are probably going to be, I hope, at a D; and then in 2006, as we complete all this stuff, we are going to jump significantly up. So you are going to kind of see, unfortunately, not much in the score, and then we will be there.

Mr. RUPPERSBERGER. There is no question the Department of Homeland Security has a lot of administrative issues that they have to deal with, you know, inheriting all these different agencies, you know, pulling them together, the funding issues. I mean, it's a very difficult job, as you know, and I understand that. Do you feel that the system that's being used now and the standards for grading are just more of a bureaucratic type of system of holding people accountable based on Homeland Security and all the issues you have, do you think it's fair? And what would you do to change that system based on where you are now and to get to the end game? Because it's not—the grade is a standard, but bottom line, we want to get to where you can provide the best national security for our country.

Mr. COOPER. Exactly. Bob West, who is our Chief Information Security Officer, and I believe very strongly that the criteria are very sound. We have no issue with the criteria. Now, Bob and I both will grumble to you and complain about the negative points that kind of in this last go-round were assessed, but we understand them and we'll live with them. What becomes most important I think is how a department like the Department of Homeland Security kind of prioritizes and applies these criteria. And you've heard, I've explained the approach that we took, I've explained a little bit of why. I believe very strongly that if the committee will allow us to stay the course, and with support of our new Secretary and Deputy Secretary, the Department of Homeland Security will indeed arrive rather quickly, although it may be fiscal year 2006, at precisely where the intent of the committee and the scorecard and FISMA represent.

Mr. RUPPERSBERGER. Do you feel that you have the money or the resources to deal with the problem.

Mr. DEFFER. I think applied in a prioritized approach, yes. Now any time—again, you know, I may get beaten up, it's OK, the worst they can do is fire me. Any time we have additional funding and resource we can move faster. But we believe that within the funding and resource that we have, we absolutely are on track to succeed.

Mr. RUPPERSBERGER. I don't know if you can answer the question—I may go back to Mr. Wilshusen, who is still at the panel. I am concerned a little bit about what is happening with respect to Justice, and especially FBI within Justice. We know some of the issues, that FBI is having a hard time in their technology area. And it seems to me we have other groups—we talked about this in the first panel, I know CIA and NSA are doing very well. And we cannot afford to have our FBI that is so important to our national security, especially domestic security, not be where they need to be.

Can you discuss some of these issues—well, I'm going to ask you the question basically. You said that Immigration was under Justice, and now they also have some issues that you are dealing with

because they are now under Homeland Security. I'm concerned that we need to really refocus and prioritize in those arenas, especially FBI. You are doing Immigration. But how can, with the problems that the FBI is having, how can we now have a grading system where the Justice Department went from I think a D or an F to a B+ or B-? Could you explain that?

Mr. DEFFER. Well, I can offer a couple of thoughts. I'm not sure I can actually explain it. But one of the things that works to——

Mr. RUPPERSBERGER. And I'm going to ask you to answer this, too, Mr. Wilshusen.

Mr. DEFFER. One of the things that works to any department's advantage is if you have less things to do and less things to accredit and certify, then within the same resource base you can accomplish a lot more.

Justice lost, if you will, a significant portion of what represented the legacy systems that weren't accredited at one point in time. We inherited them all. So I think that they——

Mr. RUPPERSBERGER. Good news for them, bad news for you, right?

Mr. DEFFER. Exactly. And that's one sense.

Now the other thing that I would offer—and again, the right person to really talk to is Zal Azmi, who is the CIO at the FBI, an extremely competent professional. Zal and I have talked a couple different times about information assurance, some of the challenges that we are sharing in exchanging information and working together, our respective agencies.

I believe that under Zal they do have the proper talent and approach, I can't really speak to the timing.

Mr. RUPPERSBERGER. Do you know if they are getting the resources to do the job, based on your conversations about it?

Mr. DEFFER. Zal and I have talked about a number of vacancies, key vacancies that Zal is working on to fill. I think that as he fills those he will be able to pick up speed.

Mr. RUPPERSBERGER. I think that is a very high priority, I would think.

Do you want to address that issue, also, Mr. Wilshusen?

Mr. WILSHUSEN. Sure. The key thing in terms of FBI and DOJ having an increased score this year was basically because of what they had reported on their FISMA report to OMB and to Congress. That score was based upon an analysis of what they had reported.

Mr. RUPPERSBERGER. Are you aware of the problems with respect to the FBI?

Mr. WILSHUSEN. I am aware with regard to issues related to DCF a Trilogy——

Mr. RUPPERSBERGER. Their technology issue.

Mr. WILSHUSEN [continuing]. That they had developed that or were in the process of developing it, and it has since been terminated. At least the operational pilots have been terminated.

Mr. RUPPERSBERGER. Do you feel they have a plan to move forward in what needs to be done to be brought up to speed?

Mr. WILSHUSEN. I don't know that because we haven't looked at that, but we have received a request to take a look at that.

Mr. RUPPERSBERGER. We sure don't want to criticize the FBI. What we want to do is give the FBI all the resources they need to

fix this problem. And again it seems to me—and we alluded to this in the first panel—when you have systems that work—and again, I can say this, I'm on the House Select Intelligence Committee, I know NSA's systems are doing well. We need to make sure we pull together, find out what is working and not working, and move forward. If it's a resource problem, we have to fix it. If it's a money problem, we have to fix it.

My time is up. Thank you for being here today.

Chairman Tom DAVIS. Well, we've kept you a long time. We appreciate everything. Anybody want to add anything, add in anything they said along the way?

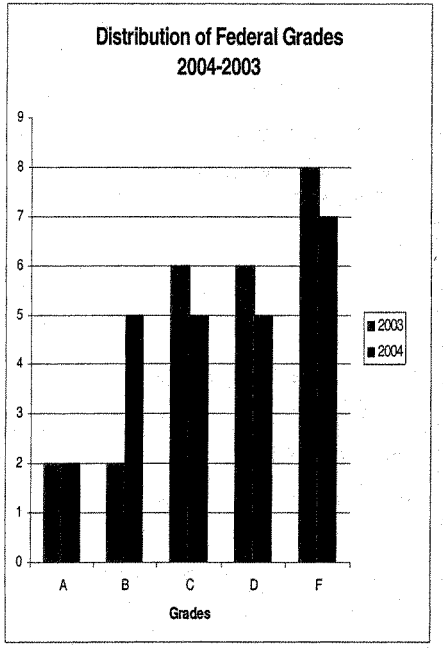
I think it has been very helpful to the committee as we move forward. I want to just thank every one of you for being here. I want to congratulate both AID and Transportation on your improvements this year. I think you've talked about this is really a team effort, it is not the CIO.

Mr. Cooper, thank you. It has been a good explanation for us. We wish you the best of luck as you move forward and appreciate the job you have done.

Thank you very much. The hearing is adjourned.

[Whereupon, at 12:03 p.m., the committee was adjourned.]

[Additional information submitted for the hearing record follows:]



FIFTH REPORT CARD

On

COMPUTER SECURITY

At

Federal Departments and Agencies

Overall Grade: D+

February 16, 2005

FEDERAL COMPUTER SECURITY REPORT CARD

February 16, 2005

GOVERNMENTWIDE GRADE 2004: D+

	2004	2003		2004	2003
AGENCY FOR INTERNATIONAL DEVELOPMENT*	A+	C-	DEPARTMENT OF STATE	D+	F
DEPARTMENT OF TRANSPORTATION	A-	D+	DEPARTMENT OF TREASURY**	D+	D
NUCLEAR REGULATORY COMMISSION	B+	A	DEPARTMENT OF DEFENSE**	D	D
SOCIAL SECURITY ADMINISTRATION	B	B+	NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	D-	D-
ENVIRONMENTAL PROTECTION AGENCY	B	C	SMALL BUSINESS ADMINSTRATION	D-	C-
DEPARTMENT OF LABOR	B-	B	DEPARTMENT OF COMMERCE	F	C-
DEPARTMENT OF JUSTICE	B-	F	DEPARTMENT OF VETERANS AFFAIRS**	F	C
GENERAL SERVICES ADMINISTRATION	C+	D	DEPARTMENT OF AGRICULTURE	F	F
NATIONAL SCIENCE FOUNDATION	C+	A-	DEPARTMENT OF HEALTH AND HUMAN SERVICES	F	F
DEPARTMENT OF THE INTERIOR	C+	F	DEPARTMENT OF ENERGY	F	F
DEPARTMENT OF EDUCATION	C	C+	HOUSING AND URBAN DEVELOPMENT	F	F
OFFICE OF PERSONNEL MANAGEMENT	C-	D-	DEPARTMENT OF HOMELAND SECURITY	F	F

* - Inspector General did not submit an independent evaluation of the agency's security management program as required by the Federal Information Security Management Act of 2002

** - No independent evaluation from the Inspector General was submitted in 2003

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