AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

FEDERAL IT SECURITY: THE FUTURE OF FISMA

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

AND THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JUNE 7, 2007

Serial No. 110–32

Printed for the use of the Committee on Oversight and Government Reform

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

U.S. GOVERNMENT PRINTING OFFICE

39–025 PDF WASHINGTON : 2008

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSISGHT AND GOVERNMENT REFORM

HENRY A. WAXMAN, California, *Chairman*

TOM LANTOS, California
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
BRIAN HIGGINS, New York
JOHN A. YARMUTH, Kentucky
BRUCE L. BRALEY, Iowa
ELEANOR HOLMES NORTON, District of Columbia
BETTY McCOLLUM, Minnesota
JIM COOPER, Tennessee
CHRIS VAN HOLLEN, Maryland
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont

TOM DAVIS, Virginia
DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
JOHN M. McHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, Jr., Tennessee
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. McHENRY, North Carolina
VIRGINIA FOXX, North Carolina
BRIAN P. BILBRAY, California
BILL SALI, Idaho
JIM JORDAN, Ohio

PHIL SCHILIRO, *Chief of Staff*
PHIL BARNETT, *Staff Director*
EARLEY GREEN, *Chief Clerk*
DAVID MARIN, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

WM. LACY CLAY, Missouri, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
JOHN A. YARMUTH, Kentucky
PAUL W. HODES, New Hampshire

MICHAEL R. TURNER, Ohio
CHRIS CANNON, Utah
BILL SALI, Idaho

TONY HAYWOOD, *Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

EDOLPHUS TOWNS, New York, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CHRISTOPHER S. MURPHY, Connecticut
PETER WELCH, Vermont
CAROLYN B. MALONEY, New York

BRIAN P. BILBRAY, California
TODD RUSSELL PLATTS, Pennsylvania,
JOHN J. DUNCAN, Jr., Tennessee

MICHAEL McCARTHY, *Staff Director*

CONTENTS

	Page
Hearing held on June 7, 2007	1
Statement of:	
Bond, Phil, president and CEO, Information Technology Association of America; Paul Kurtz, partner and chief operating officer, Good Harbor Consulting, LLC; John W. Carlson, executive director, Financial Services Roundtable/BITS; and James Andrew Lewis, director and senior fellow, Technology and Public Policy Program, Center for Strategic and International Studies	84
Bond, Phil	84
Carlson, John W.	109
Kurtz, Paul	100
Lewis, James Andrew	132
Evans, Karen S., Administrator, Office of E-Government and Information Technology, Office of Management and Budget; Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office; and Vance Hitch, Chief Information Officer, Department of Justice	10
Evans, Karen S.	10
Hitch, Vance	56
Wilshusen, Gregory C.	21
Letters, statements, etc., submitted for the record by:	
Bond, Phil, president and CEO, Information Technology Association of America, prepared statement of	86
Carlson, John W., executive director, Financial Services Roundtable/BITS, prepared statement of	112
Clay, Hon. Wm. Lacy, a Representative in Congress from the State of Missouri, prepared statement of	6
Davis, Hon. Tom, a Representative in Congress from the State of Virginia, prepared statement of	69
Evans, Karen S., Administrator, Office of E-Government and Information Technology, Office of Management and Budget, prepared statement of	12
Hitch, Vance, Chief Information Officer, Department of Justice, prepared statement of	57
Kurtz, Paul, partner and chief operating officer, Good Harbor Consulting, LLC, prepared statement of	102
Lewis, James Andrew, director and senior fellow, Technology and Public Policy Program, Center for Strategic and International Studies, prepared statement of	134
Towns, Hon. Edolphus, a Representative in Congress from the State of New York, prepared statement of	3
Wilshusen, Gregory C., Director, Information Security Issues, Government Accountability Office, prepared statement of	23

FEDERAL IT SECURITY: THE FUTURE OF FISMA

THURSDAY, JUNE 7, 2007

HOUSE OF REPRESENTATIVES, SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES, JOINT WITH THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT, COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittees met, pursuant to notice, at 2:13 p.m. in room 2154, Rayburn House Office Building, Hon. Edolpuhs Towns (chairman of the Subcommittee on Government Management, Organization and Procurement) and Hon. Wm. Lacy Clay (chairman of the Subcommittee on Information Policy, Census, and National Archives) presiding.

Present: Representatives Towns, Clay, Hodes, Davis of Virginia, and Turner.

Staff present from the Subcommittee on Information Policy, Census, and National Archives: Tony Haywood, staff director/counsel; Adam C. Bordes, professional staff member; Jean Gosa, clerk; Nidia Salazar, staff assistant; Michelle Mitchell, legislative assistant for Congressman Wm. Lacy Clay; Leneal Scott, information systems manager, full committee; Charles Phillips, minority counsel; Victoria Proctor, minority senior professional staff member; Allyson Blandford, minority professional staff member; and Benjamin Chance, minority clerk.

Staff present from the Subcommittee on Government Management, Organization, and Procurement: Michael McCarthy, staff director; Velvet Johnson, counsel; and LaKeshia Myers, editor/staff assistant.

Mr. TOWNS. The subcommittee will come to order.

Today's hearing is a joint hearing of two subcommittees of the House Oversight and Government Reform Committee on the important topic of Federal information security. We have both the Subcommittee on Government Management, which I chair, and the Subcommittee on Information Policy, led by my friend from St. Louis, Chairman Clay.

We are holding this hearing jointly because computer security presents challenges both of management and of information policy, privacy in particular. I will briefly discuss some of the management issues that I see, and then I will yield to Chairman Clay for his opening remarks.

The security of our technology has gotten a lot more attention in the past 2 years, mainly because of the serious breaches of security that have come to light. The most obvious example, of course, was the loss of a laptop computer containing sensitive personal data on millions of our Nation's veterans. Fortunately, that computer was recovered and the data was not accessed. But the episode served as a real wake-up call about how quickly and easily security can break down. Our committees' investigations learned that similar security breakdowns had occurred in every Government agency we surveyed.

These security issues are on the minds of American citizens. I hear from my constituents that they are worried about identity theft and privacy and want to know what is being done to keep their personal data safe from hackers and other criminals.

It has been 5 years now since Congress passed the Federal Information Security Management Act. This law has done a lot to create standards and accountability for our computer security, but, given our findings that security breaches are still far too common, we want to ask today what the next steps should be. What works. We would like to get that information. And what does not work? What are some new approaches we should try?

From a management point of view, there are a few specific issues I hope our witnesses can address. First, we need to know if complying with FISMA makes computer systems secure in the real world, or whether there are other factors to measure and require that would increase actual security.

No. 2: how can the Government move away from patching together security for different equipment after the fact and move toward buying equipment and systems with security already built in?

And the third: what lessons can we learn from the private sector on how to make systems more secure? Of course, the private sector has its own security problems, and we all recognize that, so we should look at what mistakes they are making, in addition to what they are doing right.

Thank you to all of witnesses that are here today. We in Congress will benefit from your advice as we consider what new legislation is needed to improve computer security.

[The prepared statement of Hon. Edolphus Towns follows:]

HENRY A. WAXMAN, CALIFORNIA,
CHAIRMAN

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

ONE HUNDRED TENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5051
FACSIMILE (202) 225–4784
MINORITY (202) 225–5074
TTY (202) 225–6852

http://oversight.house.gov

TOM DAVIS, VIRGINIA,
RANKING MINORITY MEMBER

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

OPENING STATEMENT OF CHAIRMAN EDOLPHUS TOWNS
GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT SUBCOMMITTEE

JOINT HEARING WITH THE
INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES SUBCOMMITTEE
OF THE COMMITTEE ON
GOVERNMENT OVERSIGHT AND REFORM

"FEDERAL IT SECURITY: THE FUTURE FOR FISMA"
THURSDAY, JUNE 7, 2007
2154 Rayburn House Building – 2:00 P.M.

Today's hearing is a joint hearing of two subcommittees of the House Oversight Committee on the important topic of federal information security. We have both the Subcommittee on Government Management, which I chair, and the Subcommittee on Information Policy, led by my friend from Missouri, Chairman Clay.

We are holding this hearing jointly because computer security presents challenges both of management and of information policy, privacy in particular. I'll briefly discuss some of the management issues that I see, then will yield to Chairman Clay for his opening remarks.

The security of our technology has gotten a lot more attention in the past two years, mainly because of the serious breaches of security that have come to light. The most obvious example, of course, was the loss of a laptop computer containing sensitive personal data on millions of our nation's veterans. Fortunately, that computer was recovered and the data were not accessed, but the episode served as a wake-up call about how quickly and easily security can break down. Our committee's investigations learned that similar security breakdowns had occurred in every government agency we surveyed.

These security issues are on the minds of American citizens. I hear from my constituents that they are worried about identity theft and privacy, and want to know what is being done to keep their personal data safe from hackers and other criminals.

It's been five years now since Congress passed the Federal Information Security Management Act, or FISMA for short. This law has done a lot to create standards and

accountability for computer security. But given our findings that security breaches are still far too common, we want to ask today what the next steps are. What works? What doesn't? What are some new approaches we should try?

From a management point of view, there are a few specific issues I hope our witnesses can address.

First, we need to know if complying with FISMA makes computer systems secure in the real world, or whether there are other factors to measure and require that would increase actual security.

Second, how can the government move away from patching together security for different equipment after the fact, and move toward buying equipment and systems with security already built in?

And third, what lessons can we learn from the private sector on how to make systems more secure? Of course, the private sector has its own security problems, so we should look at what mistakes they are making, in addition to what they are doing right.

Thank you to all the witnesses here today. We, in Congress, will benefit from your advice, as we consider what new legislation is needed to improve computer security.

***

Mr. TOWNS. At this time I would like to yield to the Chair of the other subcommittee that is sponsoring this hearing today, Congressman Clay.

Mr. CLAY. Thank you so much, Chairman Towns, especially for agreeing to host this joint committee with the Information Policy Subcommittee.

Let me start out by saying good afternoon. I join my good friend and colleague, Chairman Towns, in welcoming everyone to today's joint hearing to evaluate the implementation of the Federal Information Security Management Act of 2002, widely known as FISMA.

Today's hearing continues a bipartisan effort to evaluate progress under FISMA and find ways to improve our Government information security for the benefit of all Americans. Weaknesses in Federal information security threaten the operation of Federal programs and the privacy of individuals whose personal information is maintained in Government computer systems. Congress passed FISMA to require Federal agencies to adopt stronger measures to identify and minimize potential risks to the security of information and information systems.

Although important progress has been made, recent data breach incidents involving the Department of Veterans Affairs, the Internal Revenue Service, and other agencies tells us that Government information systems remain vulnerable to hackers and security breaches.

In its recent annual report to Congress on FISMA implementation efforts, the Office of Management and Budget states that progress in fiscal year 2006 was, at best, mixed. Some agencies have improved their performance under FISMA, but others, including the Department of Homeland Security and the State Department, continue to do a poor job of securing their network. Twenty-one out of 24 major agencies showed major weaknesses in their information security controls, and agency Inspectors General cite major flaws in the quality of agency certification and accreditation processes. Thus, it is clear that our current practices and policies need to be reviewed to see where improvements can be made.

I thank all of our witnesses for appearing today and look forward to your testimony.

Mr. Chairman, I yield back. Thank you.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

Opening Statement of Rep. Wm. Lacy Clay (D-MO), Chairman
Subcommittee on Information Policy, Census, and National Archives
House Committee on Oversight and Government Reform

Joint Hearing on "Federal IT Security: The Future for FISMA"

before the Subcommittee on Government Management, Organization, and Procurement and the Subcommittee on Information Policy, Census, and National Archives

June 7, 2007

GOOD AFTERNOON. I JOIN MY GOOD FRIEND AND COLLEAGUE CHAIRMAN TOWNS IN WELCOMING EVERYONE TO TODAY'S JOINT HEARING TO EVALUATE THE IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002, WIDELY KNOWN AS FISMA ("FIZZ-ma"). TODAY'S HEARING CONTINUES A BIPARTISAN EFFORT TO EVALUATE PROGRESS UNDER FISMA AND FIND WAYS TO IMPROVE GOVERNMENT INFORMATION SECURITY FOR THE BENEFIT OF ALL AMERICANS.

WEAKNESSES IN FEDERAL INFORMATION SECURITY THREATEN THE OPERATION OF FEDERAL PROGRAMS AND THE PRIVACY OF INDIVIDUALS WHOSE PERSONAL INFORMATION IS MAINTAINED IN GOVERNMENT COMPUTER SYSTEMS. CONGRESS PASSED FISMA TO REQUIRE FEDERAL AGENCIES TO ADOPT STRONGER MEASURES TO IDENTIFY AND MINIMIZE POTENTIAL RISKS TO THE SECURITY OF INFORMATION AND INFORMATION SYSTEMS.

ALTHOUGH IMPORTANT PROGRESS HAS BEEN MADE, RECENT DATA BREACH INCIDENTS INVOLVING THE DEPARTMENT OF VETERANS AFFAIRS, THE INTERNAL REVENUE SERVICE, AND OTHER AGENCIES TELL US THAT GOVERNMENT INFORMATION SYSTEMS REMAIN VULNERABLE TO HACKERS AND SECURITY BREACHES.

IN ITS RECENT ANNUAL REPORT TO CONGRESS ON FISMA IMPLEMENTATION EFFORTS, THE OFFICE OF MANAGEMENT AND BUDGET STATES THAT PROGRESS IN FY 2006 WAS, AT BEST, MIXED. SOME AGENCIES HAVE IMPROVED THEIR PERFORMANCE UNDER FISMA, BUT OTHERS, INCLUDING THE DEPARTMENT OF HOMELAND SECURITY AND THE STATE DEPARTMENT, CONTINUE TO DO A POOR JOB OF SECURING THEIR NETWORKS. TWENTY-ONE OUT OF 24 MAJOR AGENCIES SHOWED MAJOR WEAKNESSES IN THEIR INFORMATION SECURITY CONTROLS; AND AGENCY INSPECTORS GENERAL CITE MAJOR FLAWS IN THE QUALITY OF AGENCY CERTIFICATION AND ACCREDITATION PROCESSES.

THUS, IT IS CLEAR THAT OUR CURRENT PRACTICES AND POLICIES NEED TO BE REVIEWED TO SEE WHERE IMPROVEMENTS CAN BE MADE.

I THANK ALL OF OUR WITNESSES FOR APPEARING TODAY AND LOOK FORWARD TO THEIR TESTIMONY.

##

Mr. TOWNS. Thank you very much.

I would now like to yield to Mr. Turner of Ohio for his opening statement. Thank you.

Mr. TURNER. Thank you, Chairman Towns and Chairman Clay, for holding this joint oversight hearing today on information technology security and the future of the Federal Information Security Management Act.

Ranking Member Davis was the driving force behind the passage of FISMA as part of the E-Government Act in 2002. I commend his continued leadership on the issue of IT security in our Federal Government.

Breaches in IT security are not only a threat to our national security, but pose a threat to private citizens' information. In fiscal year 2006, several agencies saw potential breaches in their IT security, including the VA, the Department of Transportation, the Department of Energy, the IRS, and the Department of State. According to a September 2006, report in the Washington Post, more than 1,100 laptop computers have vanished from the Department of Commerce since 2001, including nearly 250 from the Census Bureau containing such personal information as names, incomes, and security numbers.

As a result of the work in the 109th Congress, the Subcommittee on Federalism and the Census' staff issued an interim report on the breach and Republican staff continues its investigation to this date.

I also sit on the House Veterans Affairs Committee, and, as most of you know, in May of last year we dealt with a serious potential breach in the VA's IT systems when an employee's laptop was stolen from his residence. That laptop contained the Social Security numbers of 26.5 million of our Nation's veterans. While the laptop was recovered and the data therein was not compromised, this is an example of why oversight on this topic is important.

Under then Chairman Buyer's leadership, the House Veterans' Affairs Committee held six hearings on the issue of cyber security in the VA, which culminated in the House passage of H.R. 5835, the Veterans' Identity and Credit Security Act of 2006, which incorporate provisions from this committee.

I look forward to reviewing the information that we receive from the witnesses today about FISMA's compliance, as well as a broad range of public and private sector IT security issues.

Thank you.

Mr. TOWNS. Thank you very much, Mr. Turner.

Mr. Hodes.

Mr. HODES. Thank you, Mr. Chairman.

I thank both Chairman Towns and Chairman Clay for holding this important hearing on Federal information technology security. I also appreciate the witnesses who are here today, and I look forward to your testimony on these issues.

Congress passed FISMA in part to make sure that citizens' personal information was safe with its Federal Government. In addition to protection from identity theft, security systems also ensured that the American people are receiving the most efficient service possible from their Federal agencies. But the recent data leaks which have been mentioned, including at the Department of Veter-

ans Affairs, Transportation, and Energy, as well as at the IRS, prove there are still serious flaws in the Federal Government's information defense system.

The Office of Management and Budget recently released a report stating that there were over 5,000 security incidents within Federal agencies in fiscal year 2006, up 18 percent from the previous year.

Reports of inadequate security controls at the Departments of Defense, Homeland Security, and State also raise concerns that protecting electronic data is also a significant threat to our national security.

When it comes to information security, the old phrase "good enough for Government work" does not apply.

I hope that today's hearing will shed light on the challenges facing FISMA implementation and potential solutions to those issues.

Thank you. I yield back my time, Mr. Chairman.

Mr. TOWNS. Thank you very much.

Now we will turn to the first panel. It is committee policy that all witnesses are sworn in, so please stand and raise your right hands.

[Witnesses sworn.]

Mr. TOWNS. Let the record reflect that they all responded in the affirmative. Thank you. You may be seated.

Our first panel features the experts on information security in the Federal Government. Karen Evans is the Administrator of the Office of E-Government and Information Technology at the Office of Management and Budget. She is an experienced IT professional and leads the administration's programs on information security.

Welcome to the committee.

Also, we would like to welcome Mr. Wilshusen, who is the Director of Information Security Issues at the Government Accountability Office [GAO]. He is also a long-time expert on this topic and has testified before this committee several times.

Welcome back.

Vance Hitch is the Chief Information Officer at the Department of Justice. He manages Department information and technology programs with a budget of $2.4 billion—that is B as in Boy—and has more than 30 years of experience in managing Government IT projects.

And let me note that your entire statement will be included in the record. If you could just summarize within a 5-minute period, we would certainly appreciate it, which will allow time for questions and answers.

I know you know the procedure in terms of when the yellow light comes on that is caution, and when the red light comes on, that means we hope that you will stop.

Ms. Evans, will you proceed?

STATEMENTS OF KAREN S. EVANS, ADMINISTRATOR, OFFICE OF E-GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET; GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE; AND VANCE HITCH, CHIEF INFORMATION OFFICER, DEPARTMENT OF JUSTICE

STATEMENT OF KAREN S. EVANS

Ms. EVANS. Good afternoon, Chairman Towns, Chairman Clay, and members of the committee. Thank you for inviting me to discuss the status of the Federal Government's efforts to safeguard our information and information systems. My remarks today will focus on our strategy for addressing continuing challenges, securing and protecting the information of our citizens.

OMB has taken a number of steps to improve information security and privacy through effective use of policy tools, our Government-wide management processes, and leveraging our requirements in the marketplace. Overall, Departments continue to improve their programs. The specific information has been included in the annual submission of the Federal Information Security Management Act Report to Congress and has been included in my written testimony today.

In 2006, as noted, several agencies experienced high-profile data security breaches involving personally identifiable information.

I have also included in my written statement many of the activities the administration has also taken to date to address these issues.

I would like to mention specific activities OMB is engaging now to move beyond compliance and to improve information security and privacy. Some of these initiatives include: the information technology security line of business, standard identification for Federal employees and contractors, the adoption of a common desktop security configuration, and Government-wide contracts for data encryption.

Our most recent initiative is: focus on helping agencies to procure secure software and applications. For example, we recently completed a Government-wide contract through the GSA's smart buy initiative for anti-virus software, and we are nearing completion on another smart buy contract for Federal Information Processing Standards 140–2 certified encryption tools, which will include the ability for State and local governments to also purchase these tools at the Federal Government prices from this contract.

We also have recently issued a memorandum requiring agencies to adopt common desktop security configurations for Windows XP and the Vista operating system, with a target completion date of February 1, 2008. The policy also requires secure configurations to be included in their agency procurements going forward from June 30, 2007.

We are leveraging the work that has been completed collectively and cooperatively by Microsoft, the National Institute of Standards and Technology, Department of Homeland Security, and the Department of Defense. OMB has now provided the recommended

language for the agencies to use when they are issuing new acquisitions.

The administration takes its information security and privacy responsibilities very seriously. These actions will help reduce the security incidents we have been experiencing, permit us to better respond when prevention fails, and provide us a more complete and timely view of agency performance.

Agencies spend more than $6 billion a year on controls to protect information and computer systems, and we will continue, trough our oversight and the President's management agenda scorecard process, to ensure that this money is wisely spent.

Finally, the administration intends to continue to focus on protecting the personal information of our citizens, while improving our services. An information security program, when implemented correctly, results in protection of all information, including personal information.

I look forward to working with you to improve our security and our privacy programs and welcome any suggestions you may have. I would be happy to take questions when appropriate.

[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

June 7, 2007

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

Good security and privacy are shared responsibilities. As you know, within a framework of laws developed by Congress and through direction from the President, the Office of Management and Budget (OMB) develops policies for and oversees agencies' programs to protect information security and privacy. Agencies are responsible for implementing the policies based upon the risk and magnitude of harm that would result from a breach in their security, ensuring their programs are managed to maintain risk at an acceptable level, and Inspectors General must independently evaluate effectiveness of agency programs and processes. In addition to agency responsibility, each agency employee - from rank and file employees and their supervisors to independent evaluators and overseers must be held accountable for performing their assigned responsibilities, which include the protection of information security and privacy. Security and privacy are commonly seen as separate responsibilities and programs. They are not. We see them as separate pieces of the same puzzle – personally identifiable information is an example of what to protect, while security is a program for how to protect it.

In March 1, 2007, OMB issued our fourth annual report to the Congress on implementation of the Federal Information Security Management Act (FISMA). My remarks today will focus on the progress we have made in improving the security and privacy for government information through Agencies' security and privacy programs, as well as our strategy for addressing continuing challenges. While the FISMA report characterizes our overall programmatic progress, OMB has taken a number of additional steps to improve the security and privacy of government information through effective use of policy tools and our Government-wide management processes. I will outline some of these initiatives later in my testimony.

Overall, Departments and agencies continue to improve their programs. An increasing number of agency systems have a completed certification and accreditation, a

defined risk impact level, and a tested set of security controls and contingency plans. In addition, the majority of agencies report having appropriate oversight in place for their privacy programs. However, our view of the state of government security is much the same as reflected in your Committee's annual security report card: programs require additional improvements in implementation.

Progress in Improving Agency Security Programs

This year, as in past years, OMB provided agencies specific guidance for reporting on the status and progress of their security and privacy programs. The reports provide us quantitative and qualitative performance measures to continually assess agency security and privacy programs, and are used to develop our annual FISMA report.

The FY 2006 agency FISMA reports identify progress by individual Departments and agencies in the following areas:

- Certification and accreditation of systems. This past year, the number of systems with formal management approval to operate rose from 85 percent to 88 percent. The Department of Homeland Security and Department of State have made outstanding progress in certifying and accrediting their systems. Thirteen agencies now report a certification and accreditation rate of 100% of operational systems. Based on agency reports, a higher percentage of high impact systems have been certified and accredited. This potentially demonstrates agencies are working first to secure the systems presenting the highest risk.

- Testing of security controls and contingency plans. The number of systems with completed annual testing of system controls increased by 25 percent. Agencies tested security controls for 88 percent of systems and contingency plans for 77 percent of all systems, up from 61 percent and 72 percent respectively in FY 2005. The Department of Defense (DOD) alone increased system testing by more than 30 percent.

- Security Awareness Training. Agencies reported increases in the percentage of employees receiving security awareness training and for employees with significant information security responsibilities, up 10 percent and 3 percent respectively from the prior year.

The FY 2006 agency FISMA reports reveal modest success in meeting several key privacy performance measures:

- Program Oversight. In 2006, the majority of agencies report having appropriate oversight over their privacy programs in place. All agencies report having a privacy official who participates in privacy compliance activities, although 84 percent report coordinated oversight with their IG. Most agencies report privacy training for Federal employees and contractors, with 92 percent reporting general privacy training and 84 percent reporting job-specific privacy training.

- Privacy Impact Assessments. The Federal goal is for 90 percent of applicable systems to have publicly posted privacy impact assessments (PIA). In 2006, 84 percent of applicable systems government-wide has publicly posted privacy impact assessments. 88 percent had written processes or policies for all listed aspects of PIAs.

- System of Records Notices. The Federal goal is for 90 percent of applicable systems with personally identifiable information contained in a system of records covered by the Privacy Act to have developed, published, and maintained systems of records notices (SORN). In 2006, 83 percent of systems government-wide with personally identifiable information contained in a system of records covered by the Privacy Act have developed, published, and maintained current SORNs.

Securing Agency Personal Identifiable Information (PII)

In 2006, several agencies experienced high profile data security breaches involving PII. OMB's Deputy Director for Management, Clay Johnson, testified last June before the Committee on Oversight and Government Reform and described the inter-relationship between security and privacy programs. Personally identifiable information is an example of what to protect, while security is a program for how to protect it.

As part of the agency information security program, cyber security incidents are reported to the Department of Homeland Security's (DHS') US-CERT response center. The agency agreed upon definition for reportable cyber incident includes loss or breach of PII. DHS reports 40 Departments and Agencies have reported to them over 3,900 separate security incidents involving PII to date this fiscal year (through June 5, 2007). Virtually all of these incidents resulted from "internal" problems within agencies and not external attacks on agency systems.

To help address the above issues, in May 2006 the President signed Executive Order 13402, entitled "Strengthening Federal Efforts to Protect Against Identity Theft," which created the Federal Identity Theft Task Force chaired by the Department of Justice and co-chaired by the Federal Trade Commission. On April 23, 2007, the taskforce submitted a strategic plan to the President outlining steps the Federal government can take to combat identity theft. This plan, titled "Combating Identity Theft: A Strategic Plan" is available at www.idtheft.gov. In this document, the Task Force recommended better education for Federal agencies on how to protect their data and monitor compliance with existing guidance. In this regard, OMB and DHS, through the Information Systems Security Line of Business (ISS LOB), is developing a document to outline best practices and develop a list of the most common mistakes to avoid in protecting information held by the government.

OMB issued four security and privacy policy and advisory memoranda in fiscal year 2006 which:

- directed the Senior Agency Officials for Privacy for Federal agencies to conduct a review of policy and processes, train agency employees, and report to OMB in October with their annual FISMA reports;
- asked agencies to implement certain security controls within 45 days to protect remote information, including encryption for mobile devices, two factor authentication, time out functions, and data extracts;
- required agencies to report the loss of personally identifiable information within one hour and reminded agencies of longstanding policy which requires security controls to be funded within each system; and
- provided suggested steps for planning and responding to data breaches which could result in identity theft.

In October 2006, the Inspector General (IG) community assessed agencies' status in meeting the recommendations for remote access of sensitive agency information. Agencies have made progress in verifying or ensuring the adequacy of organization policy, but much work remains. We are currently in the process of working with the IGs to obtain an updated assessment of status and in this area. The implementation challenges are not insignificant and the agencies show mixed results on OMB's request for additional actions.

On May 23, 2007, OMB issued policy M 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," which directs Federal agencies to develop and implement a risk-based breach notification policy within 120 days, while ensuring proper safeguards are in place to protect the information.

Additionally, this memorandum directs agencies to:

- review and reduce current holdings of all personally identifiable information;
- review the use of Social Security Numbers to identify instances in which collection or use of the SSN is superfluous;
- establish a plan to eliminate the unnecessary collection and use of SSNs (this plan must be implemented within 18 months);
- participate in Government-wide efforts to explore alternate personal identifiers,
- protect Federal information accessed remotely;
- develop and implement an appropriate policy outlining the rules of behavior and identifying consequences and potential corrective actions for violations; and
- train employees regarding their respective responsibilities relative to safeguarding personally identifiable information and the consequences and accountability for violation of these responsibilities.

This memorandum recognizes that safeguarding against breaches from happening in the first place has greater value than responding to breaches when they occur.

Accordingly, the Federal government should not unnecessarily collect or maintain personally identifiable information.

Continuing Challenges in Implementing FISMA

While progress has been made by most agencies, reports continue to identify a number of deficiencies in agency security procedures and practices. Deficiencies are most frequently seen in overseeing contractors, and the quality of certification and accreditation and POA&M processes.

- Maintenance of accurate system inventories and contractor oversight. IGs reported a slight decrease in the number of agencies with a system inventory over 80 percent complete, from 21 in 2005 to 20 in 2006. Though the majority of agency IGs reported inventories to be 96-100 percent complete, some agencies are still demonstrating large fluctuations in the number of systems in their inventories, both upwards and downwards. This makes it unclear whether all agencies have a handle on the universe of their information and information systems. OMB asked IGs to confirm whether the agency ensures information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and National Institutes of Science and Technology (NIST) guidelines. Through IGs' evaluation of the inventory, we will have a better sense of whether or not Agencies are securing all of their information and information technology.

- Quality of certification and accreditation and Plan of Action and Milestones (POA&M) processes. Certification and accreditation and POA&M processes are important aspects of an agency information security program to assess risks, implement controls, and track corrective actions and risk mitigation. While these processes do not "guarantee" security, they help to ensure that weaknesses in information systems and programs are identified and managed well. IGs reported an overall decrease in the quality of the certification and accreditation process from 2005, where 17 agencies were reported as "satisfactory" or better, yet the number of agencies moving to the "good" and "excellent" categories increased in 2006. OMB policy requires agencies to prepare documentation (POA&Ms) for all programs and systems where a security weakness has been found, and asks agency IGs to evaluate this process. Based on OMB analysis of IG reports, no overall progress was made except that agencies that are rated as having effective processes are more often rated as being "almost always" effective rather than "mostly" effective. OMB encourages CIOs and IGs to work together to remediate these process weaknesses, and uses the IGs independent assessment of this process as one factor in assessing an agency's status and/or progress on the President's Management Agenda scorecard.

- Assignment of a risk impact level. Agencies reported a total of 10,595 systems categorized by a risk impact level of high, moderate, low, or undetermined. The number of systems categorized increased this year from 91 percent to 93 percent.

Yet, as of October 2006, 331 agency systems and 369 contractor systems had not yet been assigned a risk impact level. OMB recognizes that in order for a system to be adequately protected, the potential level of impact that system could have to an agency must be determined. OMB will continue to measure this requirement.

In addition to deficiencies noted by the agency IGs, we have identified areas of concern through our own reviews and in consultation with other experts including the agencies and the Government Accountability Office (GAO):

- Government-wide implementation of general and job-specific privacy training for Federal employees and contractors;
- Maintenance of current PIAs and SORNs for 90 percent of applicable systems;
- Implementation of privacy policies and practices, and
- Improved oversight coordination between agencies and IGs.

Activities to Improve IT Security Performance

IT Security Line of Business

The Information Systems Security Line of Business (ISS LOB) assists agencies in identifying and consolidating common security processes and technologies to improve the Government's security and privacy performance, while also increasing efficiency and reducing cost.

Last year, the initiative facilitated a competitive and analytic process to select the Department of Defense (DoD), the Office of Personnel Management, and the Department of State (in coordination with the United States Agency for International Development) as security awareness service providers. Additionally, two agencies were selected as shared service providers to support FISMA reporting processes; the Department of Justice and the Environmental Protection Agency.

Service providers demonstrated an ability to provide information security products and services on a Government-wide and cost-effective basis. Agencies are now selecting their service providers and using them.

Standard Identifications for Federal Employees and Contractors

I would like to mention longer-term steps we are taking to increase the security of our sensitive information, computer systems, facilities, and employees. In response to an August 2004 Presidential directive, OMB led the development of a common identification standard for several million Federal employees and contractors. This directive requires all Executive branch agencies to conduct background checks on their employees and contractors before issuing them permanent government identification. The agencies are in the process of conducting these checks, and they began issuing new

identification cards in October, 2006. These cards have built-in security features to control access to Government computer systems and the Government's physical facilities.

President's Management Agenda Scorecard

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

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

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

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

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

In order to "maintain green," by July 1, 2007, agencies must meet the following security and privacy criteria:

- All systems certified and accredited;
- Systems installed and maintained in accordance with security configurations; and

- Has demonstrated for 90 percent of applicable systems a PIA has been conducted and is publicly posted; and

- Has demonstrated for 90 percent of systems with personally identifiable information contained in a system of records covered by the Privacy Act to have developed, published, and a maintained current SORN.

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

Review of Agency Information Technology Investment Requests

FISMA requires agencies to ensure information security is addressed throughout the life cycle of each information system, and several years ago OMB included this policy into Circular A-11, our primary budget guidance to the Agencies, to incorporate of the costs for security in the lifecycle of information technology capital investments.

When determining whether funding of agency investments is justified, we review whether agency capital planning documentation adequately demonstrates how each investment addresses the requirements of the FISMA, Privacy Act, OMB policy, and NIST guidelines, as appropriate. This procedure also helps agencies ensure information security management processes are integrated with agency strategic and operational planning processes.

For example, agencies must demonstrate:

- security costs are incorporated in to the life-cycle costs for each investment;
- security controls (e.g., certification and accreditation, security testing, and contingency plans) are completed and up to date;
- contractor security procedures are monitored and validated;
- security weaknesses are incorporated into the agency's plan of actions and milestones process;
- system of records notices are completed and up to date; and
- privacy impact assessments are completed, up to date, and published for the public to review.

GSA SmartBuy Initiative

Through the GSA SmartBuy initiative, we are working to help agencies procure better information security and privacy tools at a lower cost. Recently, we completed a SmartBuy for anti-virus software, and, are nearing completion on a SmartBuy for FIPS 140-2 certified encryption tools.

Adoption of Common Security Configurations

OMB recently issued policy memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," requiring agencies to adopt standard security configurations for Windows XP and VISTA by February 1, 2008. These configurations were established collaboratively by Microsoft, NIST, DHS, and DoD.

Common security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. This allows agencies to improve system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of government information.

A number of concurrent activities will further assist agency adoption of common security configurations. NIST and DHS continue to work with Microsoft to establish a virtual machine to provide agencies and information technology providers access to Windows XP and VISTA images. The images will be pre-configured with the recommended security settings for test and evaluation purposes to help certify applications operate correctly.

Additionally, OMB provided recommended language for agencies to use to ensure new acquisitions include these common security configurations and information technology providers certify their products operate effectively using these configurations.

Conclusion

I have outlined above a number of actions we are taking to demonstrate the Administration takes its information security and privacy responsibilities very seriously. These will help prevent security incidents, permit us to better respond if prevention fails, and provide us a more complete and timely view of agency performance. Agencies spend more than $6.0 billion each year on controls to protect information and computer systems. We will use the budget process to ensure this money is wisely spent and re-emphasize new spending on information technology will not be approved if sound security is not already in place for existing systems and programs. OMB encourages CIOs, Senior Agency Officials for Privacy, and IGs to work together to remediate deficiencies.

Finally, the Administration intends to focus on protecting the personal information of our citizens. Information security, when implemented correctly, results in the protection of all information, including personal information.

I look forward to working with you to improve our security and privacy programs and welcome any suggestions you have.

Mr. TOWNS. Thank you very much.
Mr. Wilshusen.

STATEMENT OF GREGORY C. WILSHUSEN

Mr. WILSHUSEN. Chairman Towns, Chairman Clay, members of the subcommittee, thank you for inviting me to testify at today's hearing on information security in the Federal Government.

For many years GAO has identified weaknesses in information security as a Government-wide, high-risk issue with potentially devastating consequences, such as intrusions by malicious users, compromised networks, and the theft of personal identifiable information. Over the past year or so, we have seen many of these consequences become reality.

Recently reporting information security incidents at Federal agencies have placed sensitive data at risk, including the theft, loss, or improper disclosure of personally identifiable information on millions of Americans, thereby exposing them to a loss of privacy and the potential harm associated with identity theft. The wide range of these incidents underscores the need for improved security practices.

Today I will discuss the weaknesses that persist in information security controls at Federal agencies, progress that the agencies have made in implementing FISMA, and opportunities to enhance the usefulness of the annual FISMA reports and independent evaluations.

Mr. Chairman, serious weaknesses continue to threaten the confidentiality, integrity, and availability of Federal systems and information. Almost all major agencies were cited by GAO or their Inspectors General or independent auditors for significant control deficiencies.

For example, 22 of the 24 agencies did not have adequate access controls in place to ensure that only authorized individuals could view, access, or manipulate data.

Even basic controls were sometimes inconsistently implemented. For example, well-known vendor supply passwords were not changed. Users were granted access privileges that exceeded their need. Network devices and services were not securely configured. Sensitive information was not encrypted, and audit logs were not adequately maintained.

Agencies also lack effective physical security controls. For instance, many of the data losses that occurred at Federal agencies were a result of physical thefts or improper safeguarding of laptops or other portable devices.

An underlying cause for these weaknesses is that agencies have not fully or effectively implemented the information security programs required by FISMA. As a result, agencies may not have the assurance that controls are in place and operating as intended to protect their information systems, thereby leaving them vulnerable to disruption, attack, or compromise.

Nevertheless, Federal agencies report steady progress in implementing FISMA control activities. For example, in fiscal year 2006 the number of major agencies that now have a substantially complete inventory increased from 13 to 18, and the number of percentages of Federal systems Government-wide that have been certified

and accredited, tested and evaluated, and have tested contingency plans all increased. The percentage of Federal employees and contractors who received security awareness increased from 81 to 90 percent, while the percentage of employees with significant security responsibilities who received specialized training also increased. However, IGs at several agencies sometimes disagreed with the agency-reported information and identified weaknesses in the processes used to implement some of these activities.

OMB has taken steps to improve the security of Federal information by recommending agencies encrypt all sensitive information on mobile computers and devices and requiring agencies to adopt common security configurations for Windows XP and Vista operating systems. If effectively implemented, these steps could strengthen agencies' controls over sensitive information.

Opportunities exist for enhanced FISMA reporting. Most of the performance metrics used for FISMA reporting measure the extent to which a control has been implemented. However, with two exceptions they don't address the effectiveness of the control. Additional information on control effectiveness or the quality of processes used to implement the controls would help agencies, OMB, and the Congress to better ascertain the state of Federal information security.

Improvements should also be made to the independent annual evaluations performed by the IGs. The IGs lacked a common approach and used varying scopes and methodologies for performing the evaluations, making comparisons across agencies over time less meaningful.

The President's Council on Integrity and Efficiency has developed a framework which might provide a more consistent approach for the evaluations.

In summary, Federal systems and information remain at risk, despite reported progress in implementing required information security controls.

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

[The prepared statement of Mr. Wilshusen follows:]

United States Government Accountability Office

GAO

Testimony
Before Congressional Subcommittees
Committee on Oversight and Government Reform
House of Representatives

For Release on Delivery
Expected at 2:00 pm EDT
Thursday, June 7, 2007

INFORMATION SECURITY

Agencies Report Progress, but Sensitive Data Remain at Risk

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO-07-935T

June 7, 2007

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-935T, a testimony before congressional subcommittees, Committee on Oversight and Government Reform, House of Representatives

INFORMATION SECURITY

Agencies Report Progress, but Sensitive Data Remain at Risk

Why GAO Did This Study

For many years, GAO has reported that weaknesses in information security are a widespread problem with potentially devastating consequences—such as intrusions by malicious users, compromised networks, and the theft of personally identifiable information—and has identified information security as a governmentwide high-risk issue.

Concerned by reports of significant vulnerabilities in federal computer systems, Congress passed the Federal Information Security Management Act of 2002 (FISMA), which permanently authorized and strengthened the information security program, evaluation, and reporting requirements for federal agencies.

In this testimony, GAO discusses security incidents reported at federal agencies, the continued weaknesses in information security controls at major federal agencies, agencies' progress in performing key control activities, and opportunities to enhance FISMA reporting and independent evaluations. To address these objectives, GAO analyzed agency, inspectors general (IG), and GAO issued and draft reports on information security.

www.gao.gov/cgi-bin/getrpt?GAO-07-935T.

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

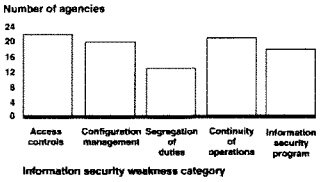
What GAO Found

Federal agencies have recently reported a spate of security incidents that put sensitive data at risk. Personally identifiable information about millions of Americans has been lost, stolen, or improperly disclosed, thereby exposing those individuals to loss of privacy, identity theft, and financial crimes. The wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches underscore the need for improved security practices.

As illustrated by these security incidents, significant weaknesses in information security controls threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. Almost all of the major federal agencies had weaknesses in one or more areas of information security controls (see figure). Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. For example, agencies did not consistently identify and authenticate users to prevent unauthorized access, apply encryption to protect sensitive data on networks and portable devices, and restrict physical access to information assets. In addition, agencies did not always manage the configuration of network devices to prevent unauthorized access and ensure system integrity, such as patching key servers and workstations in a timely manner; assign incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction; and maintain or test continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully or effectively implemented agencywide information security programs.

Nevertheless, federal agencies have continued to report steady progress in implementing certain information security requirements. However, IGs at several agencies sometimes disagreed with the agency's reported information and identified weaknesses in the processes used to implement these and other security program activities. Further, opportunities exist to enhance reporting under FISMA and the independent evaluations completed by IGs.

Information Security Weaknesses at Major Federal Agencies for Fiscal Year 2006



Source: GAO analysis.

Mr. Chairmen and Members of the Subcommittees:

Thank you for the opportunity to participate in today's joint hearing to discuss information security over federal systems. Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where the public's trust is essential. The need for a vigilant approach to information security is demonstrated by the dramatic increase in reports of security incidents, the wide availability of hacking tools, and steady advances in the sophistication and effectiveness of attack technology. Proper safeguards are essential to protect systems from malicious insiders and external attackers attempting to gain unauthorized access and obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other systems. Over the past year, federal agencies have reported numerous security incidents.

For many years, we have reported that poor information security is a widespread problem with potentially devastating consequences. In reports to Congress since 1997, we have identified information security as a governmentwide high-risk issue.[1] Concerned by reports of significant weaknesses in federal computer systems, Congress passed the Federal Information Security Management Act (FISMA) of 2002,[2] which permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies.

In my testimony today, I will summarize (1) security incidents reported at federal agencies, (2) the effectiveness of information security at federal agencies, (3) agencies' reported progress in performing key control activities, and (4) opportunities to enhance FISMA reporting and independent evaluations. In preparing for this testimony, we relied on our previous reports and ongoing work on information security at federal agencies. We also analyzed agencies'

[1]GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

[2]FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No.107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

inspectors general (IG) reports pertaining to information security; congressional reports; annual FISMA reports for 24 major federal agencies;[5] the performance and accountability reports for those agencies; and the Office of Management and Budget (OMB) FISMA guidance and mandated annual reports to Congress. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results in Brief

Recently reported information security incidents at federal agencies have placed sensitive data at risk. For example, personally identifiable information about millions of Americans has been lost, stolen, or improperly disclosed, thereby exposing those individuals to loss of privacy, identity theft, and financial crimes. The wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches underscores the need for improved security practices.

As illustrated by these security incidents, significant weaknesses in information security controls threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. Almost all of the 24 major federal agencies had weaknesses in information security controls. Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. For example, agencies did not consistently (1) identify and authenticate users to prevent unauthorized access; (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (3) establish sufficient boundary protection mechanisms; (4) apply

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

encryption to protect sensitive data on networks and portable devices; (5) log, audit, and monitor security-relevant events; and (6) restrict physical access to information assets. In addition, agencies did not always manage the configuration of network devices to prevent unauthorized access and ensure system integrity, such as patching key servers and workstations in a timely manner; assign incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction; and maintain or test continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully or effectively implemented agencywide information security programs. As a result, agencies may not have assurance that controls are in place and operating as intended to protect their information and information systems, thereby leaving them vulnerable to disruption, attack, or compromise.

Despite persistent information security weaknesses, federal agencies have continued to report steady progress in implementing certain information security requirements. For fiscal year 2006 reporting, governmentwide percentages increased for employees and contractors receiving security awareness training and employees with significant security responsibilities receiving specialized training. Percentages also increased for systems that had been tested and evaluated at least annually, systems with tested contingency plans, and systems that had been certified and accredited.[4] However, IGs at several agencies sometimes disagreed with the agency reported information and identified weaknesses in the processes used to implement these and other security program activities.

Opportunities exist for enhanced FISMA reporting and independent evaluations. Although OMB increased its reporting guidance to agencies, the metrics used do not measure how effectively agencies

[4]OMB requires that agency management officials formally authorize their information systems to process information and 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.

are performing various activities. For example, agencies report on the number of systems undergoing test and evaluation in the past year, but there is no measure of the quality of agencies' test and evaluation processes. Additionally, there are no requirements to report on certain key activities such as patch management. Further, independent annual evaluations completed by IGs lack a common approach. The scope and methodologies used by IGs varied across agencies, resulting in the collective IG community performing their evaluations without optimal effectiveness and efficiency. A common framework may provide IGs with the means to be more efficient by focusing evaluative procedures on areas of higher risk and by following an integrated approach designed to gather evidence efficiently.

Background

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. For example, resources (such as federal payments and collections) could be lost or stolen, data could be modified or destroyed, and computer resources could be used for unauthorized purposes or to launch attacks on other computer systems. Sensitive information, such as taxpayer data, Social Security records, medical records, and proprietary business information could be inappropriately disclosed, browsed, or copied for improper or criminal purposes. Critical operations could be disrupted, such as those supporting national defense and emergency services. Finally, agencies' missions could be undermined by embarrassing incidents, resulting in diminished confidence in their ability to conduct operations and fulfill their responsibilities.

Recognizing the importance of securing federal systems and data, Congress passed FISMA, which sets forth a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. FISMA's framework creates a cycle of risk management activities necessary for an effective security program, and are similar to the

principles noted in our study of the risk management activities of leading private sector organizations[5]—assessing risk, establishing a central management focal point, implementing appropriate policies and procedures, promoting awareness, and monitoring and evaluating policy and control effectiveness. More specifically, FISMA requires agency information security programs that, among other things, include

- periodic assessments of the risk;
- risk-based policies and procedures;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;
- 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;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations.

In addition, agencies must develop and maintain an inventory of major information systems that is updated at least annually.

OMB and agency IGs play key roles under FISMA. FISMA specifies that, among other responsibilities, OMB is to develop policies, principles, standards, and guidelines on information security, and is required to report annually to Congress. OMB has provided instructions to federal agencies and their IGs for FISMA annual reporting. OMB's reporting instructions focus on performance metrics such as certification and accreditation, testing of security

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

controls, and security training. Its yearly guidance also requests IGs to report on their agencies' efforts to complete their inventory of systems and requires agencies to identify any physical or electronic incidents involving the loss of, or unauthorized access to, personally identifiable information.

FISMA also requires agency IGs to perform an independent evaluation of the information security programs and practices of the agency to determine the effectiveness of such programs and practices. Each evaluation is to include (1) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems and (2) assessing compliance (based on the results of the testing) with FISMA requirements and related information security policies, procedures, standards, and guidelines. These required evaluations are then submitted by each agency to OMB in the form of a template that summarizes the results. In addition to the template submission, OMB encourages the IGs to provide any additional narrative in an appendix to the report that provides meaningful insight into the status of the agency's security or privacy program.

Incidents Place Sensitive Information at Risk

Since May 2006, federal agencies have reported a spate of security incidents that put sensitive data at risk. Personally identifiable information about millions of Americans has been lost, stolen, or improperly disclosed, thereby exposing those individuals to loss of privacy, identity theft, and financial crimes. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices. The following reported examples illustrate that a broad array of federal information and assets are at risk.

- The Department of Veterans Affairs (VA) announced that computer equipment containing personally identifiable information on approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee. Until the

equipment was recovered, veterans did not know whether their information was likely to be misused. In June, VA sent notices to the affected individuals that explained the breach and offered advice concerning steps to reduce the risk of identity theft. The equipment was eventually recovered, and forensic analysts concluded that it was unlikely that the personal information contained therein was compromised.

- A Centers for Medicare & Medicaid Services contractor reported the theft of a contractor employee's laptop computer from his office. The computer contained personal information including names, telephone numbers, medical record numbers, and dates of birth of 49,572 Medicare beneficiaries.
- The Department of Agriculture (USDA) was notified that it had posted personal information on a Web site. Analysis by USDA later determined that the posting had affected approximately 38,700 individuals, who had been awarded funds through the Farm Service Agency or Rural Development program. That same day, all identification numbers associated with USDA funding were removed from the Web site. USDA is continuing its effort to identify and contact all those who may have been affected.
- The Transportation Security Administration (TSA) announced a data security incident involving approximately 100,000 archived employment records of individuals employed by the agency from January 2002 until August 2005. An external hard drive containing personnel data, such as Social Security number, date of birth, payroll information, and bank account and routing information, was discovered missing from a controlled area at the TSA Headquarters Office of Human Capital.
- The Census Bureau reported 672 missing laptops, of which 246 contained some degree of personal data. Of the missing laptops containing personal information, almost half (104) were stolen, often from employees' vehicles, and another 113 were not returned by former employees. Commerce reported that employees were not held accountable for not returning their laptops.
- Officials at the Department of Commerce's Bureau of Industry and Security discovered a security breach in July 2006. In investigating this incident, officials were able to review firewall logs for an 8-month period prior to the initial detection of the incident, but were unable to clearly define the amount of time that perpetrators were

inside its computers, or find any evidence to show that data was lost as a result.

- The Treasury Inspector General for Tax Administration reported that approximately 490 computers at the Internal Revenue Service (IRS) were lost or stolen between January 2003 and June 2006. Additionally, 111 incidents occurred within IRS facilities, suggesting that employees were not storing their laptop computers in a secured area while the employees were away from the office. The IG concluded that it was very likely that a large number of the lost or stolen computers contained unencrypted data and also found other computer devices, such as flash drives, CDs, and DVDs, on which sensitive data were not always encrypted.
- The Department of State experienced a breach on its unclassified network, which daily processes about 750,000 e-mails and instant messages from more than 40,000 employees and contractors at 100 domestic and 260 overseas locations. The breach involved an e-mail containing what was thought to be an innocuous attachment. However, the e-mail contained code to exploit vulnerabilities in a well-known application for which no security patch existed at that time. Because the vendor was unable to expedite testing and deploy a new patch, the department developed its own temporary fix to protect systems from being further exploited. In addition, the department sanitized the infected computers and servers, rebuilt them, changed all passwords, installed critical patches, and updated their anti-virus software.

Based on the experience of VA and other federal agencies in responding to data breaches, we identified numerous lessons learned regarding how and when to notify government officials, affected individuals, and the public.[6] These lessons have largely been addressed in guidance issued by OMB. OMB has issued several policy memorandums over the past 13 months. For example, it sent memorandums to agencies to reemphasize their responsibilities under law and policy to (1) appropriately safeguard sensitive and personally identifiable information, (2) train employees on their responsibilities to protect sensitive information, and (3) report security incidents. In May 2007, OMB issued additional detailed

[6]GAO, *Privacy: Lessons Learned About Data Breach Notification*, GAO-07-657, (Washington, D.C., Apr. 30, 2007).

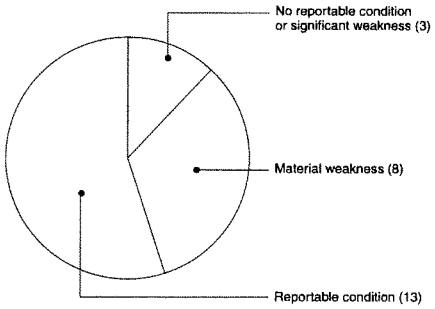
guidelines to agencies on safeguarding against and responding to the breach of personally identifiable information, including developing and implementing a risk-based breach notification policy, reviewing and reducing current holdings of personal information, protecting federal information accessed remotely, and developing and implementing a policy outlining the rules of behavior, as well as identifying consequences and potential corrective actions for failure to follow these rules.

Weaknesses Persist at Federal Agencies

As illustrated by numerous security incidents, significant weaknesses continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. In their fiscal year 2006 financial statement audit reports, 21 of 24 major agencies indicated that deficient information security controls were either a reportable condition or material weakness (see fig. 1).[7] Our audits continue to identify similar conditions in both financial and non-financial systems, including agencywide weaknesses as well as weaknesses in critical federal systems.

[7]Reportable conditions are significant deficiencies in the design or operation of internal controls that could adversely affect the entity's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements. A material weakness is a reportable condition that precludes the entity's internal controls 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.

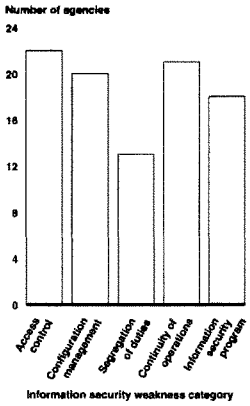
Figure 1: Agencies Reporting of Information Security Controls in Fiscal Year 2006 Financial Statement Audits



Source: GAO analysis.

Persistent weaknesses appear in five major categories of information system controls: (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and (5) an agencywide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented. Figure 2 shows the number of major agencies that had weaknesses in these five areas.

Figure 2: Information Security Weaknesses at the 24 Major Agencies for Fiscal Year 2006



Source: GAO analysis.

Access Controls Were Not Adequate

A basic management control objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modification, disclosure, or deletion of the data. Access controls, which are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities, can be both electronic and physical. Electronic access controls include the use of passwords, access privileges, encryption, and audit logs. Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft.

Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. Our analysis of IG, agency, and our own reports uncovered that agencies did not have adequate access controls in

place to ensure that only authorized individuals could access or manipulate data. Of the 24 major agencies, 22 had access control weaknesses. For example, agencies did not consistently (1) identify and authenticate users to prevent unauthorized access, (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate, (3) establish sufficient boundary protection mechanisms, (4) apply encryption to protect sensitive data on networks and portable devices, and (5) log, audit, and monitor security-relevant events. Agencies also lacked effective controls to restrict physical access to information assets. For instance, many of the data losses that occurred at federal agencies over the past few years were a result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.

Shortcomings Existed in Other Controls

In addition to access controls, other important controls should be in place to protect the confidentiality, integrity, and availability of information. These controls include policies, procedures, and techniques addressing configuration management to ensure that software patches are installed in a timely manner; appropriately segregating incompatible duties; and establishing continuity of operations planning.

Agencies did not always configure network devices and services to prevent unauthorized access and ensure system integrity, such as patching key servers and workstations in a timely manner; assign incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction; and maintain or test continuity of operations plans for key information systems. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of information.

Agencywide Security Programs Were Not Fully Implemented

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented all the FISMA-required elements for an agencywide information security program. An agencywide security program, required by FISMA, provides a framework and continuing cycle of

activity for assessing and managing risk, developing and implementing security policies and procedures, promoting security awareness and training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. Our analysis determined that at least 18 of the 24 major federal agencies had not fully implemented agencywide information security programs. Results of our recent work illustrate that agencies often did not adequately design or effectively implement policies for elements key to an information security program.

We identified weaknesses in information security program activities, such as agencies' risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. For example,

- One agency had no documented process for conducting risk assessments, while another agency had outdated risk assessments. Another agency had assessed and categorized system risk levels and conducted risk assessments, but did not identify many of the vulnerabilities we found and had not subsequently assessed the risks associated with them.
- Agencies had developed and documented information security policies, standards, and guidelines for information security, but did not always provide specific guidance on how to guard against significant security weaknesses regarding topics such as physical access, Privacy Act-protected data, wireless configurations, and business impact analyses.
- Instances existed where security plans were incomplete or not up-to-date.
- Agencies did not ensure all information security employees and contractors, including those who have significant information security responsibilities, received sufficient training.
- Our report[8] on testing and evaluating security controls revealed that agencies had not adequately designed and effectively implemented

[8]GAO, *Information Security: Agencies Need to Develop and Implement Adequate Policies for Periodic Testing*, GAO-07-65, (Washington, D.C.: October 2006).

policies for testing their security controls in accordance with OMB and NIST guidance. Further, agencies did not always address other important elements, such as the definition of roles and responsibilities of personnel performing tests, identification and testing of security controls common to multiple systems, and the frequency of periodic testing. In other cases, agencies had not tested controls for all of their systems.

- Our report on security controls testing also revealed that seven agencies did not have policies to describe a process for incorporating weaknesses identified during periodic security control testing into remedial actions. In our other reviews, agencies indicated that they had corrected or mitigated weaknesses; however, we found that those weaknesses still existed. In addition, we reviewed agencies' system self-assessments and identified weaknesses not documented in their remedial action plans. We also found that some deficiencies had not been corrected in a timely manner.

As a result, agencies do not have reasonable assurance that controls are implemented correctly, operating as intended, or producing the desired outcome with respect to meeting the security requirements of the agency, and responsibilities may be unclear, misunderstood, and improperly implemented. Furthermore, agencies may not be fully aware of the security control weaknesses in their systems, thereby leaving their information and systems vulnerable to attack or compromise. Until agencies effectively and fully implement agencywide information security programs, federal data and systems will not be adequately safeguarded to prevent disruption, unauthorized use, disclosure, and modification.

Examples Illustrate Weaknesses at Agencies

Recent reports by GAO and IGs show that while agencies have made some progress, persistent weaknesses continue to place critical federal operations and assets at risk. In our reports, we have made hundreds of recommendations to agencies to correct specific information security weaknesses. The following examples illustrate the effect of these weaknesses at various agencies and for critical systems.

- Independent external auditors identified over 130 information technology control weaknesses affecting the Department of Homeland Security's (DHS) financial systems during the audit of the department's fiscal year 2006 financial statements. Weaknesses existed in all key general controls and application controls. For example, systems were not certified and accredited in accordance with departmental policy; policies and procedures for incident response were inadequate; background investigations were not properly conducted; and security awareness training did not always comply with departmental requirements. Additionally, users had weak passwords on key servers that process and house DHS financial data, and workstations, servers, and network devices were configured without necessary security patches. Further, changes to sensitive operating system settings were not always documented; individuals were able to perform incompatible duties such as changing, testing, and implementing software; and service continuity plans were not consistently or adequately tested. As a result, material errors in DHS' financial data may not be detected in a timely manner.
- The Department of Health and Human Services (HHS) had not consistently implemented effective electronic access controls designed to prevent, limit, and detect unauthorized access to sensitive financial and medical information at its operating divisions and contractor-owned facilities.[9] Numerous electronic access control vulnerabilities related to network management, user accounts and passwords, user rights and file permissions, and auditing and monitoring of security-related events existed in its computer networks and systems. In addition, weaknesses existed in controls designed to physically secure computer resources, conduct suitable background investigations, segregate duties appropriately, and prevent unauthorized changes to application software. These weaknesses increase the risk that unauthorized individuals could gain access to HHS information systems and inadvertently or deliberately disclose, modify, or destroy the sensitive medical and financial data that the department relies on to deliver its services.

[9]GAO, *Information Security: Department of Health and Human Services Needs to Fully Implement Its Program*, GAO-06-267 (Washington, D.C.: Feb. 24, 2006).

- The Securities and Exchange Commission had made important progress addressing previously reported information security control weaknesses.[10] However, 15 new information security weaknesses pertaining to access controls and configuration management existed in addition to 13 previously identified weaknesses that remain unresolved. For example, the Securities and Exchange Commission did not have current documentation on the privileges granted to users of a major application, did not securely configure certain system settings, or did not consistently install all patches to its systems. In addition, the commission did not sufficiently test and evaluate the effectiveness of controls for a major system as required by its certification and accreditation process.
- The IRS had made limited progress toward correcting previously reported information security weaknesses at two data processing sites.[11] IRS had not consistently implemented effective access controls to prevent, limit, or detect unauthorized access to computing resources from within its internal network. These access controls included those related to user identification and authentication, authorization, cryptography, audit and monitoring, and physical security. In addition, IRS faces risks to its financial and sensitive taxpayer information due to weaknesses in configuration management, segregation of duties, media destruction and disposal, and personnel security controls.
- The Federal Aviation Administration (FAA) had significant weaknesses in controls that are designed to prevent, limit, and detect access to those air traffic control systems.[12] For example, the agency was not adequately managing its networks, system patches, user accounts and passwords, or user privileges, and it was not always logging and auditing security-relevant events. As a result, it was at increased risk of unauthorized system access, possibly

[10]GAO, *Information Security: Sustained Progress Needed to Strengthen Controls at the Securities and Exchange Commission*, GAO-06-256 (Washington, D.C.: March 27, 2007).

[11]GAO, *Information Security: Further Efforts Needed to Address Significant Weaknesses at the Internal Revenue Service*, GAO-07-364 (Washington, D.C.: March 30, 2007).

[12]GAO, *Information Security: Progress Made, but Federal Aviation Administration Needs to Improve Controls over Air Traffic Control Systems*, GAO-05-712 (Washington, D.C.: Aug. 26, 2005).

disrupting aviation operations. While acknowledging these weaknesses, agency officials stated that because portions of their systems are custom built and use older equipment with special-purpose operating systems, proprietary communication interfaces, and custom-built software, the possibilities for unauthorized access are limited. Nevertheless, the proprietary features of these systems do not protect them from attack by disgruntled current or former employees, who understand these features, or from sophisticated hackers.

- Certain information security controls over a critical internal Federal Bureau of Investigation (FBI) network were ineffective in protecting the confidentiality, integrity, and availability of information and information resources.[13] Specifically, FBI did not consistently (1) configure network devices and services to prevent unauthorized insider access and ensure system integrity; (2) identify and authenticate users to prevent unauthorized access; (3) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (4) apply strong encryption techniques to protect sensitive data on its networks; (5) log, audit, or monitor security-related events; (6) protect the physical security of its network; and (7) patch key servers and workstations in a timely manner. Taken collectively, these weaknesses place sensitive information transmitted on the network at risk of unauthorized disclosure or modification, and could result in a disruption of service, increasing the bureau's vulnerability to insider threats.
- The Federal Reserve had not effectively implemented information system controls to protect sensitive data and computing resources for the distributed-based systems and the supporting network environment relevant to Treasury auctions.[14] Specifically, the Federal Reserve did not consistently (1) identify and authenticate users to prevent unauthorized access; (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate; (3) implement adequate boundary protections to limit connectivity to systems that process Bureau of the Public Debt

[13]GAO, *Information Security: FBI Needs to Address Weaknesses in Critical Network*, GAO-07-368 (Washington, D.C.: Apr. 30, 2007).

[14]GAO, *Information Security: Federal Reserve Needs to Address Treasury Auction Systems*, GAO-06-659 (Washington, D.C.: Aug. 30, 2006).

(BPD) business; (4) apply strong encryption technologies to protect sensitive data in storage and on its networks; (5) log, audit, or monitor security-related events; and (6) maintain secure configurations on servers and workstations. As a result, auction information and computing resources for key distributed-based auction systems maintained and operated on behalf of BPD were at an increased risk of unauthorized and possibly undetected use, modification, destruction, and disclosure. Furthermore, other applications that share common network resources with the distributed-based systems may face similar risks.

- Although the Centers for Medicare & Medicaid Services had many information security controls in place that had been designed to safeguard the communication network, key information security controls were either missing or had not always been effectively implemented.[15] For example, the network had control weaknesses in areas such as user identification and authentication, user authorization, system boundary protection, cryptography, and audit and monitoring of security-related events. Taken collectively, these weaknesses place financial and personally identifiable medical information transmitted on the network at increased risk of unauthorized disclosure and could result in a disruption in service.

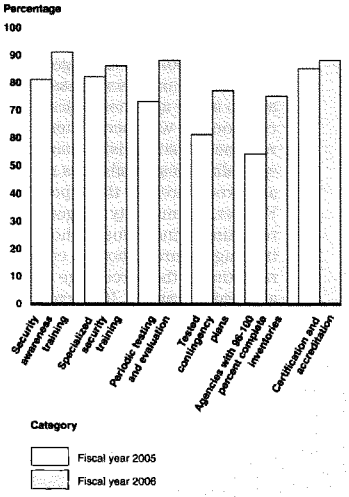
Improvements Reported in Performance Metrics, but Shortcomings Exist

Despite having persistent information security weaknesses, federal agencies have continued to report steady progress in implementing certain information security requirements. For fiscal year 2006 reporting (see fig. 3), governmentwide percentages increased for employees and contractors receiving security awareness training and employees with significant security responsibilities receiving specialized training. Percentages also increased for systems that had been tested and evaluated at least annually, systems with tested contingency plans, and systems that had been certified and

[15]GAO, *Information Security: The Centers for Medicare & Medicaid Services Needs to Improve Controls over Key Communication Network*, GAO-06-750 (Washington, D.C.: Aug. 30, 2006).

accredited. However, IGs at several agencies sometimes disagreed with the information reported by the agency and have identified weaknesses in the processes used to implement these and other security program activities.

Figure 3: Reported Data for Selected Performance Metrics for 24 Major Agencies



Source: GAO analysis of agency data.

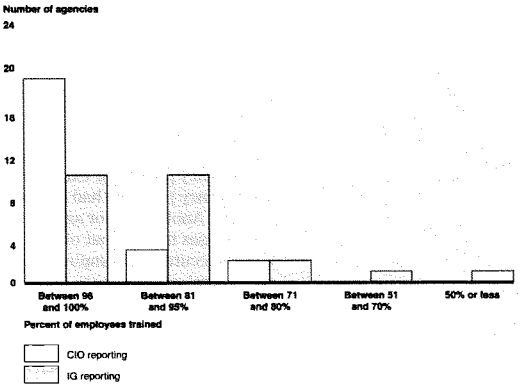
Information Security Training

The majority of agencies reported that more than 90 percent of their employees and contractors received IT security awareness training in fiscal year 2006. This is an increase from what we reported in 2006, where approximately 81 percent of employees governmentwide received IT security awareness training. There has been a slight increase in the number of employees who have security responsibilities and received specialized security training

since our last report—almost 86 percent of the selected employees had received specialized training in fiscal year 2006, compared with about 82 percent in fiscal year 2005.

Although agencies have reported improvements both in the number of employees receiving security awareness training and the number of employees who have significant security responsibilities and received specialized training, several agencies exhibit training weaknesses. For example, according to agency IGs, five major agencies reported challenges in ensuring that contractors had received security awareness training. In addition, reports from IGs at two major agencies indicated that security training across components was inconsistent. Five agencies also noted that weaknesses still exist in ensuring that all employees who have specialized responsibilities receive specialized training, as policies and procedures for this type of training are not always clear. Further, the majority of agency IGs disagree with their agencies' reporting of individuals who have received security awareness training. Figure 4 shows a comparison between agency and IG reporting of the percentage of employees receiving security awareness training. If all agency employees and contractors do not receive security awareness training, agencies risk security breaches resulting from employees who are not fully aware of their security roles and responsibilities.

Figure 4: Percentage of Employees Receiving Security Awareness Training As Reported by Agencies and IGs



Source: GAO analysis.

Periodic Testing and Evaluation of Information Security Policies, Procedures, and Practices

In 2006, federal agencies reported testing and evaluating security controls for 88 percent of their systems, up from 73 percent in 2005, including increases in testing high-risk systems. However, shortcomings exist in agencies' testing and evaluating of security controls. For example, IGs reported that not all systems had been tested and evaluated at least annually, including some high impact systems, and that weaknesses existed in agencies' monitoring of contractor systems or facilities. As a result, agencies may not have reasonable assurance that controls are implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the security requirements of the agency. In addition, agencies may not be fully aware of the security control weaknesses in their systems, thereby leaving the agencies' information and systems vulnerable to attack or compromise.

Continuity of Operations

The number of systems with tested contingency plans varied by the risk level of the system. Federal agencies reported that 77 percent of total systems had contingency plans that had been tested, up from 61 percent in 2005. However, on average, high-risk systems had the smallest percentage of tested contingency plans compared to other risk levels —only 64 percent of high-risk systems had tested contingency plans.

Several agencies had specific weaknesses in developing and testing contingency plans. For example, the IG of a major agency noted that contingency planning had not been completed for certain critical systems. Another major agency IG noted that the agency had weaknesses in three out of four tested contingency plans—the plans were inaccurate, incomplete, or outdated, did not meet department and federal requirements, and were not tested in accordance with department and federal government requirements. Without developing contingency plans and ensuring that they are tested, the agency increases its risk that it will not be able to effectively recover and continue operations when an emergency occurs.

Inventory of Systems

A complete and accurate inventory of major information systems is essential for managing information technology resources, including the security of those resources. 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 such as testing systems annually, testing contingency plans, and certifying and accrediting systems. Thus, inaccurate or incomplete data on the total number of agency systems affects the percentage of systems shown as meeting the requirements. FISMA requires that agencies develop, maintain, and annually update an inventory of major information systems operated by the agency or under its control.

The total number of systems in some agencies' inventories varied widely from 2005 to 2006. In one case, an agency had a 300 percent increase in the number of systems, while another had approximately a 50 percent reduction in the number of their systems. IGs identified

some problems with agencies' inventories. For example, IGs at two large agencies reported that their agencies still did not have complete inventories, while another questioned the reliability of its agency's inventory since that agency relied on its components to report the number of systems and did not validate the numbers. Without complete, accurate inventories, agencies cannot efficiently maintain and secure their systems. In addition, the performance measures used to assess agencies' progress may not accurately reflect the extent to which these security practices have been implemented.

Certification and Accreditation

Federal agencies continue to report increasing percentages of systems completing certification and accreditation from fiscal year 2005 reporting. For fiscal year 2006, 88 percent of agencies' systems governmentwide were reported as certified and accredited as compared to 85 percent in 2005. In addition, 23 agencies reported certifying and accrediting more than 75 percent of their systems, an increase from 21 agencies in 2005.

Although agencies reported increases in the overall percentage of systems certified and accredited, results of work by their IGs showed that agencies continue to experience weaknesses in the quality of this metric. For fiscal year 2006, ten IGs rated their agencies' certification and accreditation process as poor or failing—an increase from last year. In at least three instances of agencies reporting certification and accreditation percentages over 90 percent, their IG reported that the process was poor. Moreover, IGs continue to identify specific weaknesses with key documents in the certification and accreditation process such as risk assessments and security plans not being completed per NIST guidance or finding those items missing from certification and accreditation packages. IG reports highlighted weaknesses in security plans such as agencies not using NIST guidance, not identifying controls that were in place, not including minimum controls, and not updating plans to reflect current conditions. In other cases, systems were certified and accredited, but controls or contingency plans were not properly tested. Because of these discrepancies and weaknesses, reported certification and accreditation progress may not be providing an

accurate reflection of the actual status of agencies' implementation of this requirement. Furthermore, agencies may not have assurance that accredited systems have controls in place that properly protect those systems.

Policies and Procedures

Agencies had not always implemented security configuration policies. Twenty-three of the major federal agencies reported that they currently had an agencywide security configuration policy. Although 21 IGs agreed that their agency had such a policy, they did not agree that the implementation was always as high as agencies reported. To illustrate, one agency reported implementing configuration policy for a particular platform 96 to 100 percent of the time, while their IG reported that the agency implemented that policy only 0 to 50 percent of the time. Another IG noted that three of the agency's components did not have overall configuration policies and that other components, which had the policies, did not take into account applicable platforms. If minimally acceptable configuration requirements policies are not properly implemented and applied to systems, agencies will not have assurance that products are configured adequately to protect those systems, which could increase their vulnerability and make them easier to compromise.

Security Incident Procedures

Shortcomings exist in agencies' security incident reporting procedures. According to the US-CERT[16] annual report for fiscal year 2006, federal agencies reported a record number of incidents, with a notable increase in incidents reported in the second half of the year. However, the number of incidents reported is likely to be inaccurate because of inconsistencies in reporting at various levels. For example, one agency reported no incidents to US-CERT,

[16]FISMA charged the Director of OMB with ensuring the operation of a federal information security center. The required functions are performed by DHS's US-CERT, which was established to aggregate and disseminate cybersecurity information to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection.

although it reported more than 800 incidents internally and to law enforcement authorities. In addition, analysis of reports from three agencies indicated that procedures for reporting incidents locally were not followed—two where procedures for reporting incidents to law enforcement authorities were not followed and one where procedures for reporting incidents to US-CERT were not followed. Several IGs also noted specific weaknesses in incident procedures such as components not reporting incidents reliably, information being omitted from incident reports, and reporting time requirements not being met. Without properly accounting for and analyzing security problems and incidents, agencies risk losing valuable information needed to prevent future exploits and understand the nature and cost of threats directed at the agency.

Remedial Actions to Address Deficiencies in Information Security Policies, Procedures, and Practices

IGs reported weaknesses in their agency's remediation process. According to IG assessments, 16 of the 24 major agencies did not almost always incorporate information security weaknesses for all systems into their remediation plans. They found that vulnerabilities from reviews were not always being included in remedial actions. They also highlighted other weaknesses that included one agency having an unreliable process for prioritizing weaknesses and another using inconsistent criteria for defining weaknesses to include in those plans. Without a sound remediation process, agencies cannot be assured that information security weaknesses are efficiently and effectively corrected.

Opportunities Exist to Enhance Reporting and Independent Evaluations

Periodic reporting of performance measures for FISMA requirements and related analysis provides valuable information on the status and progress of agency efforts to implement effective security management programs; however, opportunities exist to enhance reporting under FISMA and the independent evaluations completed by IGs.

Limited Assurance of the Quality of Agency Processes

In previous reports, we have recommended that OMB improve FISMA reporting by clarifying reporting instructions and requesting IGs to report on the quality of additional performance metrics. OMB has taken steps to enhance its reporting instructions. For example, OMB added questions regarding incident detection and assessments of system inventory. However, the current metrics do not measure how effectively agencies are performing various activities. Current performance measures offer limited assurance of the quality of agency processes that implement key security policies, controls, and practices. For example, agencies are required to test and evaluate the effectiveness of the controls over their systems at least once a year and to report on the number of systems undergoing such tests. However, there is no measure of the quality of agencies' test and evaluation processes. Similarly, OMB's reporting instructions do not address the quality of other activities such as risk categorization, security awareness training, or incident reporting. OMB has recognized the need for assurance of quality for agency processes. For example, it specifically requested that the IGs evaluate the certification and accreditation process. The qualitative assessments of the process allows the IG to rate its agency's certification and accreditation process using the terms "excellent," "good," "satisfactory," "poor," or "failing." Providing information on the quality of the processes used to implement key control activities would further enhance the usefulness of the annually reported data for management and oversight purposes.

Reporting Does Not Include Aspects of Key Activities

Currently, OMB reporting guidance and performance measures do not include complete reporting on certain key FISMA-related activities. For example, FISMA requires each agency to include policies and procedures in its security program that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. As we previously reported,[17] maintaining up-to-date patches is key to complying with

[17]GAO, *Information Security: Continued Action Needed to Improve Software Patch Management*, GAO-04-706 (Washington, D.C.: June 2, 2004).

this requirement. As such, we recommended that OMB address patch management in its FISMA reporting instructions. Although OMB addressed patch management in its 2004 FISMA reporting instructions, it no longer requests this information. As a result, OMB and the Congress lack information that could identify governmentwide issues regarding patch management. This information could prove useful in demonstrating whether or not agencies are taking appropriate steps for protecting their systems.

Office of Inspector General Evaluations of Implementation Varied

Although the IGs conducted annual evaluations, they did not have a common approach. We received copies of all 24 IG FISMA template submissions and 20 IG FISMA reports.[18] For these efforts, the scope and methodology of IGs' evaluations varied across agencies. For example:

- According to their FISMA reports, certain IGs reported interviewing officials and reviewing agency documentation, while others indicated conducting tests of implementation plans (e.g. security plans).
- Multiple IGs indicated in the scope and methodology sections of their reports that their reviews were focused on selected components, whereas others did not make any reference to the breadth of their review.
- Several reports were solely comprised of a summary of relevant information security audits conducted during the fiscal year, while others included additional evaluation that addressed specific FISMA-required elements, such as risk assessments and remedial actions.
- The percentage of systems reviewed varied; 22 of 24 IGs tested the information security program effectiveness on a subset of systems; two IGs did not review any systems.
- One IG noted that the agency's inventory was missing certain Web applications and concluded that the agency's inventory was only

[18]Two agencies—the Departments of Education and Justice—did not complete full reports for fiscal year 2006; the audit reports for two other agencies—the Departments of Commerce and Veterans Affairs—are still considered "draft."

0-50 percent complete, although it also noted that, due to time constraints, it was unable to determine whether other items were missing.

- Two IGs indicated basing a portion of their template submission solely on information provided to them by the agency, without conducting further investigation.
- Some reviews were limited due to difficulties in verifying information provided to them by agencies. Specifically, certain IGs stated that they were unable to conduct evaluations of their respective agency's inventory because the information provided to them by the agency at that time was insufficient (i.e. incomplete or unavailable).

The lack of a common methodology, or framework, has culminated in disparities in audit scope, methodology, and content. As a result, the collective IG community may be performing their evaluations without optimal effectiveness and efficiency. A commonly used framework or methodology for the FISMA independent evaluations is a mechanism that could provide improved effectiveness, increased efficiency, and consistency of application. Such a framework may provide improved effectiveness of the annual evaluations by ensuring that compliance with FISMA and all related guidance, laws, and regulations are considered in the performance of the evaluation. IGs may be able to use the framework to be more efficient by focusing evaluative procedures on areas of higher risk and by following an integrated approach designed to gather evidence efficiently. Without a consistent framework, work completed by IGs may not provide information that is comparable for oversight entities to assess the governmentwide information security posture.

In summary, as illustrated by recent incidents at federal agencies, significant weaknesses in information security controls threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. Almost all major agencies exhibit weaknesses in one or more areas of information security controls. Despite these persistent weaknesses, agencies have continued to report steady progress in implementing certain information security requirements. However, IGs sometimes disagreed with the agency's

reported information and identified weaknesses in the processes used to implement these and other security program activities. Further, opportunities exist to enhance reporting under FISMA and the independent evaluations completed by IGs.

Mr. Chairman, this concludes my statement. I am happy to answer any questions at this time.

Contacts and Acknowledgments

If you have any questions regarding this report, please contact me at (202) 512-6244 or wilshusen@gao.gov. Other key contributors to this report include Jeffrey Knott (Assistant Director), Larry Crosland, Nancy Glover, Min Hyun, and Jayne Wilson.

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

Mr. TOWNS. Thank you very much.
Mr. Hitch.

STATEMENT OF VANCE HITCH

Mr. HITCH. Good afternoon and thank you, Mr. Chairman and members of the committee, for the invitation to speak to you today.

As the Chief Information Officer for the Department of Justice, I am proud to discuss the accomplishments of the Department in the area of information security and FISMA compliance during my 5 years of service at the Department.

Your Honor has asked me to discuss DOJ's efforts to comply with FISMA and the role the CIO Council plays in addressing Government-wide security challenges.

In my role as the CIO, I develop IT security policies, procedures, and tools, and then coordinate their implementation across many components. However, there are aspects of IT security which are not covered by FISMA, and I try to play the role of both mentor and facilitator to help our components balance mission-specific defensive security along with compliance-related security.

My testimony today will cover both what the Department does to ensure compliance and what we do to improve our defensive security posture across all of our 40 components within the Department of Justice.

DOJ has received a grade of A-minus for FISMA compliance, and we are very proud of this accomplishment. The majority of work, and therefore the credit, belongs to the many information technology specialists supporting over 200 FISMA reportable systems that we have. However, we at DOJ want to go beyond compliance and to support our components with mission-specific defensive security.

Today's world of cyber attacks has changed. A denial of service attack is no longer viewed as a significant accomplishment in the hacker community. Hackers now have more ambitious goals, such as placing explodable code on computers, or key-logging, to capture user-entered information. Many of the attacks come from foreign countries and criminal enterprises both here and abroad.

When I first became the CIO at DOJ, DOJ had a small security group within our policy office. One of my first organizational changes was to introduce a corporate level chief information security officer and to set up an IT security office. Our initial efforts focused on establishing a basic security program and developing a means to track and report progress back to OMB.

An obvious initial need was to bring on good people with a background in IT security. We hired from other agencies and also recruited people from the private sector. We also utilized the National Science Foundation's Cyber Corps program and have continued to hire personnel from this valuable initiative.

Once we had the right people on board, our next focus was to increase awareness and training. Our security staff updated and improved our system inventory and enhanced our policies relating to certification and accreditation and patch management. Once these basics were in place, we pushed ourselves to improve our efficiency and effectiveness. Included in this effort was the new standardized method for all components to report incidents to a centralized DOJ

computer emergency readiness team, which then had the responsibility of coordinating with the US-CERT. Our security team worked with the components to choose Department-wide tools for scanning and logging events across the networks.

Another key component of this phase was reaching on a standardized desktop and laptop configuration for our Department-wide office automation program. This move not only improved our IT security, but also better leverages our significant buying power.

As the Department moves forward, we are heavily influenced by the very significant and numerous losses of PII—personally identifiable information—that have occurred in both the Government and the private sector. DOJ is addressing the protection of PII by modifying our policies related to laptops, thumb drives, and other IT tools.

In future efforts, we will be focusing on operationalizing the policies and processes included in the new systems or in updates that we make to existing systems. Most importantly, we want to move beyond FISMA's identification of vulnerabilities to confirming the completion of security corrective actions.

We intend to insert new language in our life cycle development policies and our new contracts and into our C&A business processes. We are planning to implement a Justice security operations center by building off the work already done by the FBI. This JSOC will house the CERT team and will also house the security engineering staff to support the components in both emergency and non-emergency tasks. This will give us improved situational awareness.

The CIO Council is an outstanding group of individuals who meet to discuss a wide range of issues affecting the entire Government IT community. It is a great forum to further understand different perspectives on pending policies or legislation.

The Council also endorsed the idea of an IT security line of business, and recently DOJ was selected by OMB to run an information security line of business.

The long-term success of the IT security program at DOJ depends on much more than achieving a high FISMA grade. We are shifting our focus to defending our missions, which is more than just the systems. It is important to remember that security is a balance of mission, threat, vulnerability, cost, and compliance.

My customers in law enforcement, our attorneys and our correctional officers, expect reliable and secure collaboration capabilities. As we build new systems and upgrade our older systems, security is a crucial piece of the solution.

I encourage Congress to continue to support its Government-wide efforts such as US-CERT, the CIO Council, and Cyber Corps, which enriched our capabilities by bringing talented people together to share information and solutions.

The fight is an ever-changing fight, and we all must stay focused on the new threats and the new vulnerabilities.

Thank you for your time this afternoon. I will be very happy to answer any questions you may have.

[The prepared statement of Mr. Hitch follows:]

Department of Justice

TESTIMONY

OF

VANCE E. HITCH

DEPUTY ASSISTANT ATTORNEY GENERAL
AND CHIEF INFORMATION OFFICER
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION,
AND PROCUREMENT, AND THE
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS,
AND NATIONAL ARCHIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

"FEDERAL IT SECURITY: THE FUTURE FOR FISMA"

PRESENTED ON

JUNE 7, 2007

Vance E. Hitch
Chief Information Officer
U.S. Department of Justice

TESTIMONY BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION AND PROCUREMENT AND THE SUBCOMMITTEE ON INFORMATION POLICY, CENSUS AND NATIONAL ARCHIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES
June 7, 2007

Good afternoon and thank you, Mr. Chairman and Members of the Committee, for the invitation to speak to you today. As the Chief Information Officer for the Department of Justice, I am proud to discuss the accomplishments of the Department in the area of Information Security and FISMA-compliance during my five years of service at the Department. You have asked me to discuss DOJ's efforts to comply with FISMA and the role the CIO Council plays in addressing government-wide security challenges.

Introduction

Before I describe what the Department has done with regards to FISMA, this subcommittee should understand the complex relationship between our components. The relationship is similar to a large corporation with multiple companies and brands. In the corporate world, where I worked for 29 years, headquarters introduces mandates and recommendations and then enforces these mandates and recommendations as appropriate. FISMA is a mandate and we take the responsibility of enforcement seriously. However, there are aspects related to IT security which are not covered by FISMA, and in my role as Department CIO, I try to play the role of mentor and facilitator, to help the components balance mission-specific defensive security and compliance-

related security. Also, our Office of Inspector General plays an independent, but cooperative role in monitoring and testing the Department's compliance with FISMA and informing the Department of problems. My testimony today will cover both what the Department does to ensure compliance and what we do to improve our defensive security posture across all of the 40 components within DOJ.

The Department of Justice has received a grade of A- for FISMA compliance, and we are very proud of this accomplishment. The majority of the work, and therefore the credit, belongs to the many information technology (IT) specialists supporting our over 200 FISMA-reportable systems. DOJ now has a good foundation, but that is not good enough. We must not be complacent in our highly-rated compliance. We at DOJ want to go beyond compliance and support our components with mission-specific, defensive security. Today's world of cyber attacks has changed. A denial of service attack is no longer viewed as a significant accomplishment in the hacker community. Hackers now have more ambitious goals, such as placing exploitable code on personal and government computers (i.e. key logging) to capture user-entered information. They are in pursuit of data, with the end goal of obtaining an advantage to enhance their criminal behavior. Some also intend to cause disruption to government activities by corrupting, changing, copying or deleting data. Attacks are no longer simply about the thrill of "getting in"; rather, many of the attacks come from foreign countries and criminal enterprises here and abroad.

As DOJ moves forward, our efforts will focus on "operationalizing" security into our day-to-day IT activities, so that we are doing more than complying with FISMA. This requires system owners to put in place tools and processes to protect both the

perimeter and the core, as one would do if they were trying to protect a military base. I will provide some other examples of what we plan to do later in this testimony.

DOJ's Path to an A-

When I first became CIO, DOJ had a small security group within our policy office focused on its IT systems. One of my first organizational changes was to introduce a corporate level Chief Information Security Officer (CISO) and we recruited our CISO out of the Department of Defense. Our initial efforts (Phase 1) focused on establishing a basic security program and developing a means to track and report progress back to OMB. At the same time, I was busy implementing the steps necessary to enable me to carry out my responsibilities under the Clinger-Cohen Act across my entire organization. An obvious initial need was the demand for good people with a background in IT security. DOJ hired from other agencies and also recruited people from the private sector. We also recognized the value of the National Science Foundation's Scholarship for Service Cyber Corps Program and have continued to hire personnel from this valuable initiative. Once we had the right people on board, our next focus was to increase awareness and training. DOJ staff updated the required training materials, built the tracking system and began enforcing security awareness training requirements for all IT system administrators and users of DOJ systems. My senior staff also had to work hard to ensure component senior staff recognized the importance of IT security. My staff and I conducted many briefings for component and Department senior management in order to educate them on the real threats posed to the Department and the actions necessary to mitigate those threats. In addition, our security staff updated and improved our system inventory, and enhanced policies relating to Certification and

Accreditation (C&A) and Patch Management. Finally, we re-vamped the scorecard we use internally to track FISMA progress across the Department.

Once the basics were in place, we pushed ourselves to improve on our efficiency and effectiveness in IT security in Phase 2. Included in this effort was a new standardized method for all components to report incidents to a centralized DOJ Computer Emergency Readiness Team (CERT), which then had the responsibility of coordinating with US-CERT at the Department of Homeland Security. Our security team worked with the components to choose standard Department-wide tools for scanning and logging events across all the networks. By utilizing the same tools, we improved the ease with which the components report and share data with our headquarters staff. Another key component to our Phase 2 effort was reaching agreement on a standardized desktop and laptop configuration for our Department-wide JCON[1] program. It should be noted that this effort was accomplished one year before OMB issued new acquisition guidance related to Microsoft Windows desktops. Our components deserve credit for reaching agreement on this difficult topic. They realized that the good of the whole outweighed the needs of the individual. Compromise is never easy, but the numerous IT stakeholders pushed hard to agree on a standard and this new standard now allows DOJ to buy PCs in bulk for the enterprise at significant savings to the entire Department.

The Department currently sits at the end of Phase 2 but before I tell this sub-committee what we are going to do in Phase 3, I will address the news stories about losses of Personally Identifiable Information (PII) and the impact it has had on DOJ and other agencies. These are the type of stories that keeps CIOs up at night. As a result of

[1] Justice Consolidated Office Network.

these incidents and the guidance issued by Clay Johnson (OMB Deputy Director for Management), DOJ is addressing the protection of PII by modifying policies related to laptops, thumb drives and other IT tools. New initiatives have been put in place to define clear reporting procedures, escalation procedures and guidance pertaining to the handling of PII incidents. In addition to changing our policies and procedures, we are also looking at ways to enforce positive security behavior. Our privacy and security staffs are working together with OCIO to ensure the appropriate handling of all PII-related incidents. My staff is evaluating methods to protect systems and databases containing PII, as well as other tools that can further defend the Department from the intentional or accidental loss of sensitive data.

In our FISMA Phase 3 efforts, we are focusing on "operationalizing" the security efforts, whereby the policies and processes are included in new systems or updates that we make. Most importantly, we want to move beyond FISMA's identification of vulnerabilities to confirming the completion of security corrective actions in our systems where we have previously identified weaknesses. We intend to insert new language into our life-cycle development policies, our new contracts and into our C&A business process requirements. Our hope is that the security teams will be viewed as a "value-add" to the development process, rather than a hurdle that each project must overcome. The way we do this is through conducting executive-level security training and by hiring technically competent security professionals. Our teams will then involve the security professionals early in the system's life-cycle and make them a part of the development team, so that when the solution is ready the security checks are in place and roll-out can occur.

We also are implementing a Justice Security Operations Center (JSOC), by building off the work already done by the FBI. This JSOC will house the CERT team and also the security engineering staff to support the components in both emergency and non-emergency tasks. Project teams and individual users will have a single place to call to avoid confusion and help prevent a small problem from growing into a much larger problem. Proactive real-time monitoring across the DOJ networks will allow the JSOC to provide real-time analysis of suspicious incidents and initiate the appropriate response. This monitoring will help provide situational awareness across the Department to enable the prevention of attacks moving from one system to another. Once the JSOC is operational, my office will focus on measurements to ensure that we are looking at business-driven metrics to prove the value of the security program and the JSOC.

CIO Council

The CIO Council is an outstanding group of individuals who typically meet monthly to discuss a range of issues affecting the entire government IT community. It is a great forum to further understand different perspectives on pending policies or legislation. It is also a great place to share ideas across agencies. The Council plays an important role in shaping ideas and policies that have a significant impact on government operations, beyond just the system side of running a large agency. The Council also endorsed the idea of an IT security line of business. DOJ submitted a proposal and was selected by OMB to run a comprehensive FISMA reporting solution for the Information System Security Line of Business (ISS LOB). The DOJ solution includes automated tools and program management processes for identification

of an Agency's inventory of systems, the verification of secure system configurations, and proof of annual system testing. In addition, the solution assists users in developing plans of action and milestones to correct known security weaknesses. In this capacity, we plan on assisting many agencies as they strive to improve their FISMA scores.

Path Forward

The long term success of the IT security program at the Department depends on much more than achieving a high FISMA grade—that is, much more than achieving the baseline. We are shifting our focus to defending our missions, which includes more than just the systems. It is important to remember that security is a balance. This balance of mission, threat, vulnerability, and cost must now also include compliance. Compliance is important. It is important to verify that we are covering the basics, but we must balance these routine tasks with the job at hand. We rely on the CISOs to protect our mission operators by protecting our networks, our data, and our communications. My customers in law enforcement, our attorneys, and our correctional officers expect reliable and secure collaboration capabilities. As we build new systems and upgrade older systems, security is a crucial piece of the solution. The CIO Council is the forum where we help find common solutions to common problems. I encourage Congress to continue its support of government-wide efforts such as US-CERT, the CIO Council, and Cyber Corps, which enrich the capabilities of each agency by bringing talented people together to share information and solutions. New security initiatives such as the NIST Security Content Automation Program will help us validate our systems in an automated fashion, allowing agencies to apply security dollars to building secure systems and defending their missions. This fight is an ever-changing fight. It is

important to ensure that all agencies stay focused on new threats and new vulnerabilities.

Thank you for your time this afternoon. I will be happy to answer any questions you have.

Mr. TOWNS. Thank you.

Let me thank all three of you for your testimony. We will now move to the question period.

I am the sponsor of a bill that would regulate spyware, which passed the House yesterday. The reason for the bill is the complaints I have about spyware, not just from consumers but also from large companies that have to deal with it. One computer manufacturer has said that problems related to spyware cause most of their customers' complaints. Another company has said that spyware accounts for about 50 percent of all tech support calls.

Dealing with spyware is adding hundreds of millions of dollars in costs to companies. My question is: how much money and time do computer experts in the Government spend keeping spyware off Government computers?

Let me just go right down the line with you, Ms. Evans.

Ms. EVANS. Mr. Towns, I can't answer the specific question as it relates to spyware, because that is one piece in a comprehensive program. What we do track from an OMB perspective and what we look at from a cost perspective is ensuring that they take proper precautions within each of the investments. So we are capturing the information of what agencies intend to spend and plan to spend on security, and it has been increasing every year.

For the President's budget that was submitted that is currently under review now, the fiscal year 2008 budget, it is anticipated that included in that is $6 billion for the Federal Government as a whole to deal with information security/information protection.

Mr. TOWNS. Thank you.

Mr. WILSHUSEN. And I also can't comment directly on the cost associated with searching for and cleansing systems from spyware. I can say that it is an issue and that often spyware is quite difficult to identify on a system, so it does take some effort to identify it and then to rid it from the system, and so there is a cost associated with time and resources to do that.

Mr. TOWNS. Right.

Mr. HITCH. Likewise, I can't comment on the specific cost, but I would agree with you that it is a very large problem, and just a general problem of bugs and whether they are malicious or inadvertent that are in the software that we all use are a huge problem. We spend a tremendous amount of money on what we call patch management, which is basically implementing patches that have been found to problems within the software that we all buy.

So what I think part of the solution in the future is—and I know that OMB is very much active in this and I am working along with the CIO Council on a committee which is working on this problem right now—is to go back in the supply chain and to talk to the software vendors about their processes that they use to develop the software, making sure that they are rigorous and have certification or at least standards for them to meet before we buy their software.

The other answer is to kind of put language in our contracts which ensure that we are protected from those kind of things and have penalties when we find something that is untoward.

Mr. TOWNS. Thank you. Thank you very much.

Mr. WILSHUSEN. And if I may add, sir, I would agree with that, because one of the critical causes for most of the weaknesses we identify, or many of the weaknesses we identify on our information security reviews is the fact that systems and operating systems are not configured securely, and that patches are not installed in a timely manner, and we are able to exploit those vulnerabilities in order to increase the level of access on a particular audit, and it is one of the root causes for many of the problems that Federal agencies face in implementing their security.

Mr. TOWNS. All right.

Let me ask you, and I guess we will start with you, Ms. Evans, do the FISMA reports measure results or just how effective the agency can complete the paperwork exercise?

Ms. EVANS. Mr. Chairman, this is a complicated question, and that is why I wanted to have my remarks, and I specifically said going beyond compliance. If an agency chooses to just comply, that they view it as a paperwork exercise and look at the metrics and the activities that we have, then it will generate reports and the agency will not be secure. They will not have good management practices in place. They may have good metrics that are reported in because they will have good numbers, and that is why it is critical that we are working with the Inspectors General to have the quality aspect be reviewed of those management processes.

So what we are really trying to do is get beyond compliance. If you really just look at the letter of the law and look at what is there, you could generate an environment where the agency is just cranking out reports so that we can review those. That would not be representative of a secure program.

But if it is properly implemented, the framework with it, and really focusing on the risk and the information that you have, and having the quality of your processes evaluated, then FISMA is measuring what a good program would have, and so that is why, through our oversight, we are working with the agencies so that we can move them beyond a compliance type of "I have to get this report in to OMB and in to Congress," and really focus on the results of securing the information that they are collecting.

Mr. TOWNS. Yes.

Mr. WILSHUSEN. And if I may add, I would also say that I agree with what Ms. Evans has said in that if agencies are using this process as a paperwork exercise just in order to comply with the law, then they are missing the benefit that FISMA offers, because FISMA is based on sound information security principles, and the agencies should be more concerned about implementing the processes behind some of the metrics that are being used.

As I mentioned in my opening remarks, many of the performance measures that are now being used to measure implementation of FISMA are based on merely implementing the control. It does not address or reflect the effectiveness of those controls. That is why I believe the metrics and the reporting procedure under FISMA should further address the effectiveness of controls that are being implemented, not just whether or not a control has been implemented.

Mr. TOWNS. Right.

We have been joined by the ranking member of the full committee, Mr. Davis of Virginia. At this time I would like to yield 5 minutes to the ranking member from Virginia, Mr. Davis.

Mr. DAVIS OF VIRGINIA. Thank you very much. I ask my opening statement be put in the record.

[The prepared statement of Hon. Tom Davis follows:]

Opening Statement of Ranking Member Davis
Committee on Oversight and Government Reform
Subcommittee on Information Policy, Census, and National Archives and
Subcommittee on Government Management, Organization, and Procurement
Hearing on "*Federal IT Security: The Future for FISMA*"
June 7, 2007

Good afternoon. The two subcommittees are meeting this afternoon to review FISMA, the Federal Information Security Management Reform Act. I sponsored FISMA, and it was enacted into law on December 17, 2002, as title III of the E-Government Act of 2002. FISMA lays out the framework for annual IT security reviews, reporting, and remediation planning at federal agencies. I appreciate the interest of these subcommittees in this important federal management law.

We all know information technology drives our economy and helps the federal government operate with greater efficiency at lower costs. But, we also know government systems are prime targets for hackers, terrorists, hostile foreign governments, and identity thieves.

For bad guys, exploiting information security weaknesses might be as good as running drugs.

Security threats come in varied forms – and present a real challenge. Agencies have to balance demands to share information yet safeguard privacy. At the same time, we ask them to consolidate infrastructure and applications. And the explosion of mobile computing doesn't make it easier – sometimes the threat is just carelessness, like leaving a laptop in your unlocked car. One of the best ways to meet the information security challenge is to have strong, yet flexible, protection policies in place. We want agencies to actively protect their systems – instead of just reacting to the latest threat. We need to give people the tools to think on their feet.

When it comes to information security, the federal government can and should be the leader. FISMA requires each agency to create a comprehensive risk-based approach to agency-wide information security management. It is intended to make security management an integral

part of an agency's operations and to ensure we are actively using best practices to secure our systems.

Sure, the law has its critics – mainly from failing agencies and those who misunderstand what it was designed to do. Certainly, we want to avoid a "check the box" mentality. We need to incentivize strong information protection policies. We need to pursue a goal of security rather than compliance. The FISMA process is a good one, but we'll always ask if we can make it better – and again, I appreciate the attention we are giving FISMA today.

As most of you know, for the past several years, we have been assigning "security grades" to federal agencies and an overall "security grade" to the federal government. FISMA requires an annual independent evaluation of agency information security practices, usually performed by the IG. The agency and IG reports are submitted to Congress and OMB. These mandated reports are used to compile the

grades. In April, I announced, the overall government grade for FY2006 is a C-, indicating slow but steady improvement from past years.

We are seeing an overall improvement in federal information security. In some cases, agencies which have struggled in the past have made significant progress in complying with OMB's guidance. For instance, DHS now has a complete inventory of its systems, which is vital to good information security. You can't protect what you don't know you have. But agencies must remain vigilant as threats and vulnerabilities increase. Specifically, the reports indicate the number of systems reported and the annual testing of security controls and contingency plans have increased. And agencies have also dramatically improved incident reporting.

2006 marks the first time OMB's guidance required agencies to provide performance measures for the privacy protection of personal information. This is a vital addition to the FISMA reports, given the numerous high profile information security breaches at federal agencies

last year, including the widely publicized events at the Department of Veterans Affairs.

But additional progress is needed in developing effective security plans and milestones to measure the progress of those plans. More improvement is needed in how systems are configured from a security standpoint and for training for employees with significant information security responsibilities.

I intend to explore ways to provide an incentive through the scorecard process to agencies that effectively configure their systems with security in mind. For example, as agencies move to Microsoft Vista, bonus points could be awarded to agencies that take certain steps toward secure configurations. And there may be other additions we should consider – the testimony today should be a valuable source of good ideas.

We must remain proactive. Accordingly, earlier this week I initiated a "survey" of federal agencies as part of my continuing work to ensure the federal government effectively and efficiently manages its information technology resources and protects the privacy, reliability, and integrity of its information systems. We developed a series of questions to assess how agencies are implementing key IT laws, including FISMA, and the influence of agency chief information officers. CIOs play a vital role in implementing these IT laws and ensuring the IT investment and security decisions are consistent with the missions and goals of federal agencies.

Not long ago, we learned a British hacker finally will be extradited to Northern Virginia to face justice. He was charged with hacking into 100 DOD and NASA computers causing $700,000 in damages more than five years ago – which shows the cost, damage, and delay we face if we have to deal with information security problems after the fact. And just recently, we learned of the devastating coordinated cyber

attacks on Estonia. Our systems are attacked daily, and it is only a matter of time before we face our own cyber pearl harbor.

Again, I am pleased we are having a hearing today on this critical issue, and I look forward to working with all stakeholders to improve government-wide information security.

Mr. DAVIS OF VIRGINIA. I apologize I wasn't here earlier. I have a bill pending upstairs in another subcommittee. I am going to have to go back and forth.

Ms. Evans, let me start with you. What changes or improvements is your office proposing for the 2007 FISMA guidance? Do you plan to issue new or updated guidance regarding Circular A–130?

Ms. EVANS. Right now the draft guidance is out for the agencies to review. We are open to consideration for changes that could occur in that. Pretty much right now we are holding them steady, but really looking to the effectiveness of the measures and the quality of the processes.

Mr. DAVIS OF VIRGINIA. OK. Federal information security has been high on the GAO risk list for several years. What are you doing to address the areas of weakness that they have identified and that would remove the Government-wide information security from the list? How are we attacking this? And is there anything legislatively that we need to do to give you additional tools?

Our biggest fear is that we pass these laws, we have annual report cards. Everybody's sitting here fat, dumb, happy. If you ask the average Member what FISMA is, they think it is a new cola or something. They are really not into this. But the minute you get something approaching a cyber Pearl Harbor or something everybody is going to be pointing fingers and saying what did you do about it. So I am asking: what are we doing about it at this point?

Ms. EVANS. Well, we are moving beyond compliance. Chairman Towns just asked the question about FISMA and the reporting and the metrics and are we just in a paperwork exercise or are we really achieving the results that were intended by the legislation going forward. I feel the legislation is sound. I know you introduced a modification which deals with breach, and that also obviously needs to be addressed as far as notification to citizens and entities. However, I really believe where we are at right now is in the execution of what was intended with the law. We have gotten the basic foundation in place, but we have to get agencies really focused on what is the result intended—having good, sound management practices in place, using the tools that we have.

For example, with us spending $65 billion in information technology—and Mr. Hitch hit on this—we should be very demanding of the industry about what we need to have built into our applications, what the software should have, not making things that are more convenient for system administration types of activities and having those open so that is easier to maintain, but actually having that shut down where agencies have to make a conscious decision and balance that risk.

So I really think that we need to improve the execution of what we are doing, what was intended by the law, and in that way you can get the quality and assess the quality.

Mr. DAVIS OF VIRGINIA. Is there an issue as we ask our managers to do more and more, not just with FISMA but a whole variety of new jobs we give them, where we probably should be adding funding, or from an appropriations perspective are we doing enough to back this up, or are we just saying this is another box

to check, we expect you, with your limited time, to just add this to the list, which forces a number of difficult choices.

My experience has been managers are focused on accomplishing the mission. This is more cost avoidance, and it tends to be more check the box.

Do we need to do a better job of funding it in certain areas, and are we getting the right input from Government to do that?

Ms. EVANS. Well, the way that our policy is set up, sir, is for agencies to really look at the services they are doing and then ensuring that security and privacy and the cost to maintain that is built into the investment up front. If an agency is in a compliance mode and they view FISMA and the reporting as a check mark exercise, then when something happens or the proper precautions aren't put in place it is always more costly to go back in afterward and fix things. So we really are viewing from our capital planning process, our budgeting process, how all of this is set up, that agencies really look at this in the beginning. It is one of many responsibilities that everyone has when you are going forward to provide a service for the citizen or internally for businesses or what you are doing.

Mr. DAVIS OF VIRGINIA. I just want to get my last question in.

Mr. Hitch, let me just ask you, does the OMB guidance allow for an accurate measurement of the status of an agency's IT security program? Are you getting appropriate guidance, do you think?

Mr. HITCH. I have to say I give FISMA good grades overall. I think it has helped me through the years to give visibility to IT security, to make sure that management understands the criticality of it, and so forth, and gives me a little bit of backing when I go for funds and so forth.

I do think the bar has gone up each year, and I think that is appropriate. I think the bar should continue to go up, because the general level of IT security in the Government is better.

As I said in my opening statement, the direction that we are going—and I think that is the direction FISMA will go—is more operational aspects of making sure that we are implementing all the controls that we need to implement.

I mentioned our security operations center. Situational awareness is the other thing. Right now we are aware when we have incidents, but the question is are we aware soon enough to minimize the risk, to minimize the impact of a specific incident, to tell other components within our organization that this situation has arisen, and to mitigate the overall impact of it. So we are going for situational awareness and we are going for making sure that we are addressing all of the items in our programs, is what we call it, the items where we found vulnerabilities, to fix them. Because one of the things that a C&A, which is measured by FISMA, makes you do is to create a program of action to milestones to say you are going to fix them, it leaves it to your judgment whether or not you are going to let the system continue to operate.

What we have found is we are always aware. When an auditor points out that there is a problem in a system, we are always aware of it because we have done our homework and we have done these analyses and so forth, but we haven't fixed them all. We are fixing them in order of priority based on how significant they are,

what we think the risk of them is. So we are going to really focus on trying to get those pro-ams down and get as many of the risks as we can accomplished.

Mr. CLAY [presiding]. Thank you. The gentleman from Virginia's time has expired.

I recognize the gentleman from New Hampshire, Mr. Hodes.

Mr. HODES. Thank you, Mr. Chairman.

As a recent Member of Congress, I am just beginning to get my hands around the dimensions of the issues that we are discussing here today, and the reports that you have provided and the testimony are very helpful, so I appreciate that.

Has anybody done a study that would tell us or help us quantify the kind of dollar losses the Federal Government is suffering as a result of the issues that we are dealing with today in terms of lost productivity, lost time, lost hardware, lost software, what it is costing us on an annual basis to deal with security breaches and other problems that, if we were in a perfect world, we wouldn't have to deal with?

Mr. WILSHUSEN. We have not done such a review and we have not been requested to do such a review, but we would be willing to work with you and your staff if you would like to have one done.

Mr. HODES. Because I noted someone testified that there was $6 billion annually being spent for controls over computer systems, and my guess would be that we are losing significantly more money than that in the Government for lack of compliance and lack of ability to meet all the goals that we are trying to meet.

Mr. WILSHUSEN. The cost could be significant. I know with the VA theft of last year there was testimony that, at the time when the laptop had not been recovered, that the VA was considering providing credit monitoring and other services to the veterans. At some of the hearings they said it could cost anywhere from between, like, $30 to $100 per service member that was affected. When you multiply that by 26.5 million members, that is a big chunk of change.

Mr. HODES. I understand that, based on reports from the Inspectors General of each agency that were published during 2006, only 19 of 25 agencies reported to have an effective strategy in place to remedy security weaknesses. I am hoping we are making improvements. But in order for these agencies to provide services, many agency information systems are interoperable.

Am I correct in understanding that we really are dealing with the weakest link in the chain; that if one agency is deficient, then the entire system is really brought down to the level of that agency?

Ms. EVANS. Yes, sir, that is the simplest answer, that we are as strong as our weakest link. That is why we are taking steps beyond just the reporting and looking at the metrics, and things such as the standard desktop configuration and having that deployed across the entire Federal Government raises the bar, and then also reduces our time to patch so that it will raise the security overall. So these are execution steps now that we are in because of the exact situation that you just described.

Mr. HODES. Now, I would like to just think outside the box for a moment. Given where we are today and given the variability that

I have heard in terms of how agencies are doing—and it sounds, Mr. Hitch, like the DOJ is doing a commendable job and that you have placed an enormous emphasis on doing what you need to do to bring things up to snuff in terms of your information, and I understand that the CIOs are meeting regularly. Is there a point person, one point person who is helping to manage the issues around information security and the compliance with FISMA that we have, or is it spread around the Government? And do we need some person to take control of this and help direct all these efforts, or is what we have in place adequate?

Ms. EVANS. Sir, I will take the first shot at that.

Mr. HODES. OK.

Ms. EVANS. I would say that the point person for the administration from a policy perspective and a coordination perspective is myself. The reason being is I am also the Director of the CIO Council. So I work directly with the Department of Homeland Security, which manages our US-CERT operation, and also does the operational aspects and has Government-wide looking across the board from an operational perspective.

What we are doing from a budget perspective and then analyzing several tools that I have with, say, for example, the information security line of business and the infrastructure line of business, we are bringing those together so that we can think outside the box.

For example, every agency has a network, and your example of the weakest link, is it necessary for every agency to maintain a presence on the Internet? If you don't have a strong enough staff to fully man it 24 by 7, be aware of it, like Mr. Hitch has described, maybe that agency should be getting some of its services and its expertise from another agency.

We have identified across the board that information security professionals are a mission critical need within the Federal Government. We have identified how many we have onboard, how many we need to have across the Federal Government, and we are managing and leveraging those resources all the way across from people to the actual hardware and services that we procure. So my office puts together the policies and then analyzes the investments and the requests that come in and then make a recommendation so that the President's budget will reflect those policies and then the agency's ability to implement those.

Mr. HODES. And, No. 1, do you have enough resources? And I always hear in all these committee hearings, no, we never have enough resources, but you may. And, No. 2, is there any legislation that we need to pass to make FISMA work better and address this issue?

Ms. EVANS. Well, the President's budget, sir, reflects his priorities accordingly, and so the agencies then budget for this, and that would be in there as the risk-based approach as they go forward. I would say we have the resources that we need, $65 billion, $6 billion in this area is a lot of money that is being spent, so we need to use it appropriately.

I have really looked at the FISMA legislation and I really feel that the tenets, the principles, the things that are there are the right framework, and Congress had it right when they passed it. What we really have to look at is the agencies' execution, and look-

ing at the guidance that we are providing from this, looking at the policies of how we have interpreted some of that legislation, and work with you to enhance those so that we can get to the results that were intended.

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

Mr. CLAY. Thank you.

Let me ask Ms. Evans, does OMB require agencies to specifically account for information security in agency IT acquisition plans through the Circular A–11 processes?

Ms. EVANS. Yes, sir, they are supposed to. Mr. Chairman, they are supposed to address those in the major business cases. That is part of what is evaluated when they send what we call an exhibit 300. That is looked at in conjunction with the annual reports that the agencies do that we get from FISMA and from the IG's review, so we look at all of that information across the board when we are analyzing what the agencies are asking for and how they are planning to spend their money.

Mr. CLAY. And do you think that they are spending it in a way that protects taxpayers' investments and that is the best use of that money, or is it patchwork throughout the Government?

Ms. EVANS. I would say that the agencies are really attempting to do the best that they can. What we have the opportunity from my level is to look across the board, and so things such as—and I am going to go back on a Government-wide contract for data encryption. We can see that all agencies are requesting that. We put out the policy that agencies should have that. We are following up from things that are already there.

What we can do from my office, in conjunction with the General Services Administration, is give stronger guidance to the agencies and say we will use and leverage all our buying power over here. So things like getting a Government-wide contract, and then also extending it out to State and local governments, because they have the same issues that we do.

Looking at things like the Microsoft configuration, agencies are spending a lot on operations because you have to patch. So if we raise that and we built that into the procurement, so now you can centrally manage patching and you can distribute it faster, you can reduce some of the resources that you are spending on these daily operations and move them more into mission-specific types of activities like Mr. Hitch was talking about earlier.

Mr. CLAY. Yes. Mr. Hitch, did you have something to add?

Mr. HITCH. Well, I would just add, what Ms. Evans was talking about was at the OMB level when you submit a 300 on a system. You have to kind of check off a box and basically say that you are aware of the importance of IT security and you have in your investment enough money to cover IT security when you do this.

Down at the Department level, at DOJ, we have something called the DIRG, the departmental IT—or the U-Board. In that process you look at all of these projects as they are coming along, right from the very inception when they are first brought up and when requirements are done all the way through the contracting process through implementation. We, likewise, check IT security as part of our overall review at each checkpoint. We check it at the

budget process checkpoint and then we check it at the implementation checkpoint.

So through our processes I am trying to make sure that we are actually implementing IT security when we are actually building the systems.

I would like to pick up on a point that was made earlier, however, and that is a lot of the answer has to be a balanced approach of dealing with the systems we have now and making reasonable and intelligent choices as to what we are going to fix about those systems and the vulnerabilities in those, and then getting it earlier into the pipeline as we are building new systems to make sure that we are preventing these same errors from happening and us having to deal with them 5 and 10 years from now, because it is actually more costly to fix these vulnerabilities in their existing systems than it is to take the prudent steps necessary to prevent them from being in the systems that we are developing.

So we have to go back in the system development pipeline as we are developing the systems, and also with the products that we are using in our systems that are coming from the private sector.

Mr. CLAY. OK. Let me ask Mr. Wilshusen, in your recent report on the information security controls at the FBI indicates that there are significant weaknesses throughout the agency's networks. Can you define what the major weaknesses are——

Mr. WILSHUSEN. Sure.

Mr. CLAY [continuing]. And the necessary steps to correct the problems?

Mr. WILSHUSEN. Right. We looked at a critical internal network at the FBI and we found that the FBI did not consistently configure their network servers and devices securely. We found that they did not identify and authenticate users in an appropriate manner or enforce the principle of least privilege when assigning authorizations to users. We also found that they did not apply strong encryption or log, audit, and monitor activity over the network appropriately. And, finally, we found that they did not patch their servers in a timely manner.

All of this collectively increased the risk to insider vulnerability, so to the insider threat.

Mr. CLAY. Do you believe that agency procurement activities are adequately incorporating security into their IT budgets? Is there effective planning done by agencies during the front end of systems integration and development processes?

Mr. WILSHUSEN. Do you mean generally or in this specific instance?

Mr. CLAY. Generally.

Mr. WILSHUSEN. Generally I would say that is an area that needs improvement in that agencies do need to focus on identifying their security requirements up front, early in the development life cycle process, in order to assure that they are being addressed as the development process continues.

Mr. CLAY. How about in this particular case with the FBI?

Mr. WILSHUSEN. In this particular case we found that these weaknesses I think were more of a matter of management attention or in terms of assuring that the controls were not implemented in a timely manner. For example, we found that to not have a com-

plete inventory or current inventory of the network devices and/or identifying they had some issues with system interconnectivity issues, as well. In many cases, their testing and evaluation process was not very good because we identified vulnerabilities that they did not know about or identify during their test and evaluation processes on that network.

Mr. CLAY. OK. Thank you.

Mr. Hitch, anything to add on that one?

Mr. HITCH. Well, I would just add that I think when you actually do a specific review of any system you are going to find some vulnerabilities, and hopefully we have identified them and are at least aware of them and are about to have a plan to fix them or have at least made a temporary decision that, based on the overall risk and the other compensating controls, that we are willing to live with that, at least until we can get the money to fix that particular thing.

Mr. CLAY. Let me ask you to describe for us your work on the Federal CIO Council, specifically as it relates to cyber security and privacy issues. Are there specific activities on the way to address the widespread information security weaknesses at different agencies throughout the Government?

Mr. HITCH. Yes. I think the CIO Council is a very useful group in terms of the activity they pursue, particularly to IT security. There is a Best Practices Committee within the Federal CIO Council that IT security is one of the items that is very high on their agenda. In fact, this year they are going to have a cyber security day, where all the agencies are going to participating in terms of coming in and, from a training standpoint, as well as demonstration and best practices standpoint, talking about finding out the best and latest in IT security.

The Federal CIO Council, as I mentioned earlier, is also—and I am the representative on a committee to look into the pipeline process, from where the software manufacturers are producing software that we then use, all the way up through its implementation and its disposal. After we are finished with it, what do we do with it to make sure that it doesn't create any residual risk after we are finished with the systems?

So I think there are a number of initiatives that are happening on the Federal CIO Council that are very much aimed at IT security.

Mr. CLAY. Let me ask you to describe for us the flaws in your agency's oversight which led to the failure of the virtual file sharing program within the Trilogy modernization.

Mr. HITCH. OK. The virtual case file situation happened a number of years ago and, in fact, I would have to say, in conjunction with Ms. Evans, I think I was a part of the process that led to the shutting down of that process, because we felt that it was flawed. The management was flawed and the contracts that were a key part of that process were flawed.

Mr. CLAY. The vendors?

Mr. HITCH. The failure, yes.

Mr. CLAY. Yes.

Mr. HITCH. And therefore we felt that continuing to work on that was throwing good money after bad, and so we actually shut it

down. Those flaws were many. It was contracted improperly. The FBI did not have the appropriate management team in place and the skills that it kind of assumed through that contracting strategy in order to manage that contract. They, by definition, assumed a systems integration role and a project management role. So there were many issues with that, and that is why we shut it down. And when we are moving forward with a new generation, we have tried to address all of those issues.

Mr. CLAY. Let me thank this entire panel for their responses.

We are in the process of voting now on the floor. I will dismiss this panel, and then when we come back we will temporarily recess while votes are occurring. When we come back, we will swear in panel two. Thank you all for being here today.

We are temporarily in recess.

[Recess.]

Mr. CLAY. The joint hearing will come to order.

Let me thank Chairman Towns first, and I will now introduce our second panel of witnesses.

Mr. Phillip J. Bond serves as the president and chief executive officer of the Information Technology Association of America, representing 325 leading software, Internet, telecommunications, electronic commerce, and systems integration companies. His previous Government service includes serving as an Under Secretary of the U.S. Department of Commerce and Chief of Staff to former Commerce Secretary Don Evans.

Welcome, Mr. Bond.

Mr. Paul Kurtz is a partner and COO of Good Harbor Consulting, LLC, and is a recognized cyber security and homeland security expert. He previously served in senior positions on the White House's National Security and Homeland Security Councils under Presidents Clinton and Bush, and as the executive director of the Cyber Security Industry Alliance.

Welcome to the committee.

Mr. John Carlson serves as the executive director of BITS, where he focuses on information and security issues, business continuity, planning, and outsourcing risk issues for BITS financial institution members. Prior to joining BITS he worked for 9 years at the Office of the Comptroller of the Currency in a variety of roles, including Acting Director, Deputy Director, and Senior Advisor of the Bank Technology Division.

Thank you for being here, Mr. Carlson.

Mr. James Andrew Lewis directs the Technology and Public Policy Program at the Johns Hopkins Center for Strategic and International Studies and is a senior fellow. Previously he was a career diplomat who worked on a range of national security issues, including several bilateral agreements on security and technology.

Welcome to you also, Mr. Lewis.

Gentlemen, welcome to all. It is the policy of the committee on Oversight and Government Reform to swear in all witnesses before they testify. Would all of you please stand and raise your right hands?

[Witnesses sworn.]

Mr. CLAY. Let the record reflect that all of the witnesses answered in the affirmative.

Each of you will have 5 minutes to make an opening statement. Your complete written testimony will be included in the hearing record. The yellow light indicates that it is time to sum up. The red light indicates your time has expired.

Mr. Bond, we will begin with you.

STATEMENTS OF PHIL BOND, PRESIDENT AND CEO, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA; PAUL KURTZ, PARTNER AND CHIEF OPERATING OFFICER, GOOD HARBOR CONSULTING, LLC; JOHN W. CARLSON, EXECUTIVE DIRECTOR, FINANCIAL SERVICES ROUNDTABLE/BITS; AND JAMES ANDREW LEWIS, DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND PUBLIC POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

STATEMENT OF PHIL BOND

Mr. BOND. Thank you, Chairman Clay, and thank you to the subcommittees for this opportunity for ITAA to testify and talk about FISMA, an effort we have been involved in from the beginning, so commendations to the subcommittees.

In our view, FISMA brought unprecedented and much needed attention to the information security challenges of the Federal Government. Importantly, too, the legislation recognized that to solve that challenge we needed the very best of the private sector involved in coming up with the solution. In part, that is because the dynamic nature of today's rapidly evolving threats demands innovation by the private sector and those who hold so much of the network in private hands. So as the threat evolves, so must FISMA implementation over time.

We have been pleased to see the general trend that agencies are improving in this regard, but agree with the earlier statement from the gentleman from New Hampshire that it is not good enough for Government work. That is exactly right.

We believe that measurement processes can be improved to yield better results, that we can emphasize preparedness versus after-the-fact response; in effect, that FISMA could be raised to another level, or FISMA 2.0, if you will.

As providers of the information systems and security solutions, we will continue to help to the maximum extent possible.

I would like to assure you that our members take very seriously their responsibilities in this regard in providing effective products and solutions to the Government. We see ourselves as partners in the mission.

In turn, Government agencies should be encouraged to consider the very latest innovations from the private sector in this space. We have seen instances when compliance is used as an excuse, if you will, to discount the very latest in technology from the private sector.

Very quickly, software as a service is a good example of this. Some of the assumptions in FISMA and the standards behind it cause those in the agencies who are looking at compliance to say that is new, that architecture isn't assumed here, and so I won't do that. We believe removing barriers to innovation is one of six recommendations I would make very quickly to the committee: Re-

moving barriers to innovation for improvements in FISMA; reaffirming the agency information security program approval process feature to make sure that the plans aren't just on paper, but there are processes and resources behind them; third, to ensure that CIOs and chief information security officers are positioned appropriately, with necessary authority behind them. There may be some specific authorization and appropriation things we would want to talk about to make sure that they are positioned, authorized, and resourced.

Fourth, to enhance Federal cyber risk management by requiring at least an annual risk assessment by the agencies that incorporates classified information and the latest from the private sector. We know that there are some agencies who are not equipped to receive classified briefings, and yet they must build risk assessments.

Fifth, harmonize and enhance the audit and oversight. This was referenced earlier by the witnesses that the IGs in GAO need to come at this in a harmonized way. We support that, and perhaps NIST would be in a position to do some training in that regard.

Sixth, to expand Federal cyber response capabilities and update FISMA, frankly, and its procedures to reflect the fact that the Department of Homeland Security has been created in the meantime, and its involvement with the US-CERT program.

So we commend the committee. We believe Federal information security can be stronger, that we can have a FISMA 2.0, if you will, if we refine and improve the metrics—Ms. Evans referenced that a little bit, I think, focusing more on results than mere compliance—and embracing the partnership with the private sector.

Thank you.

[The prepared statement of Mr. Bond follows:]

Statement of

Phillip J. Bond
President and CEO
Information Technology Association of America

Concerning

Federal IT Security: The Future for FISMA

Before the

Subcommittee on Government Management, Organization, and Procurement
and
Subcommittee on Information Policy, Census and National Archives

Committee on Oversight and Government Reform
U.S. House of Representatives

June 7, 2007

Good afternoon, Chairman Waxman, Ranking Member Davis, Chairman Clay, Chairman Towns, Ranking Member Bilbray, Ranking Member Turner, and Members of the Subcommittees. My name is Phil Bond, and I am president and CEO of the Information Technology Association of America. Thank you for giving me the opportunity to present the IT industry's views on federal IT security and the future of the Federal Information Security Management Act (FISMA).

ITAA has more than 325 member companies and affiliations with over 16,000 companies across the U.S. through a strategic partnership with 40 regional associations. ITAA is also the secretariat of the World Information Technology and Services Alliance (WITSA), a network of IT industry associations from 69 economies around the world. Our member companies range from the smallest IT start-ups to the largest industry leaders in the fields of Internet, software, IT services, digital content, systems integration, telecommunications, and enterprise solutions. We are a leading voice on issues of importance to our industry, including information security, government procurement, tax and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy and consumer protection, government IT procurement, human resources, and e-commerce policy.

ITAA's track record in addressing issues related to information security is well documented and we maintain a robust program specifically focused on the area. Additionally, many of our member companies provide information technology, managed security, and systems integration services to the federal government. We have been involved in the efforts to improve the information security in federal departments and agencies for over a decade. ITAA supported FISMA when it was proposed, and I would like to commend this committee and, in particular, Ranking Member Davis for his extraordinary efforts toward its enactment and implementation.

The Subcommittees should be applauded for taking up this review of FISMA and its future. I look forward to this opportunity to work with you to update and improve upon the law and its implementation. This hearing sends a clear signal that you understand that information technology – and our use of it – is not static and that we must continually assess our needs and capabilities. It also makes clear your appreciation for the fact that information security is not a snapshot in time; just as our information technology needs evolve over time, so do the threats to and vulnerabilities in our ever-advancing information infrastructures. Given this dynamic environment, it is our collective responsibility to continue to assess those needs; to update the mechanisms we are using to assess our risks; and to ensure improvements in the security of our government networks.

In my testimony, I will (1) highlight key benefits of FISMA, (2) address the current state of information security in the federal government and identify specific challenges, (3) discuss the roles and responsibilities of IT solutions providers, and (4) provide a set of recommendations for enhancing FISMA – in policy and in practice.

Benefits: FISMA Fundamentally Improved Government-wide Processes and Practices

FISMA fundamentally improved security among the federal agencies by focusing attention on information security and providing a comprehensive framework for ensuring the effectiveness of

information security controls over information resources that support federal operations and assets. The Act recognized the highly networked nature of the federal computing environment and provided for effective government-wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities.

Further, FISMA recognized that the IT industry would play a key role in protecting government information security and specifically acknowledged that:

> *commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector.*[1]

I emphasize this because federal information security is an area in which the government must depend upon the best of private sector technology products and services to meet the public sector mission.

FISMA was carefully architected to drive the development and maintenance of the controls required to protect federal information and information systems and provide a mechanism for improving oversight of federal agency systems. As such, FISMA made notable improvements by:

- defining roles and responsibilities for the Office of Management and Budget (OMB), the National Institutes of Standards and Technology (NIST), and agency Chief Information Officers (CIOs) and Inspector Generals (IGs);
- creating processes for identifying and categorizing the risk level of agencies (FIPS 199);
- establishing minimum security controls (FIPS 200 and SP 800-53); and
- improving accountability with annual auditing and reporting requirements.

Federal Information Security and IT Security Challenges

Federal agencies are operating in one of the most complex environments in history. Agencies own, operate, and oversee diverse enterprises that must comply with a range of information security requirements related to the various types of information they handle. In addition to balancing these requirements, agencies must secure these enterprises against a highly dynamic threat environment. When FISMA, and its predecessor the Government Information Security Reform Act (GISRA), were first developed, the public and private sector enterprises were struggling to improve network security and defend against threats from worms, viruses, and denial of service attacks. Since then, we have seen a significant shift from such relatively loud and noisy attacks to stealthy, more sophisticated, targeted application attacks and social engineering methods that seek to steal identities and sensitive data, such as those that recently disrupted government operations in Estonia.[2] FISMA has created an important foundation for

[1] Federal Information Security Management Act,Title III of the E-Government Act of 2002 (P.L. 107-347).
[2] See Appendix A

security. But, in light of these and other evolving threats and emerging technologies, we recognize that successful information security is a continuous process and, as a result, must also evolve and change over time.

With FISMA's annual examination requirements and the resulting annual report card, Congress continues to keep the agencies' feet to the fire to ensure at least annual reporting of information security efforts. And, we were pleased to see improvements in the grades that many of the federal agencies recently received as a result of the 2006 FISMA examinations. The grades do represent a certain level of security improvements by virtue of agencies' compliance with the FISMA requirements.

However, we are concerned that the current process puts an emphasis on compliance that may not reflect positive contributions to real information security and focuses on failures after the fact. What we really need is an on-going program or set of programs that works to ensure consistent, effective security measures and interim improvements in the agency's IT architecture, policies, and procedures. As the grades indicate, the agencies are widely divergent with regard to their compliance and those grades could better measure effective, on-going security measures.

Let me provide a couple of examples where FISMA metrics could be refined and improved. One of the categories in the annual grading criteria, worth two full letter grades, is on certification and accreditation, a key first step especially in the early days of FISMA. Today however, under the certification and accreditation process, risk is measured, documented, accepted, and controlled, but not necessarily mitigated. Therefore, it is theoretically possible for all of an agency's systems to be certified and accredited and not actually be secure because the most pressing risks to the agency's information systems and sensitive data were not fully identified or addressed. Another example is awareness and training for agency personnel, an annual requirement worth a full letter grade in the FISMA scoring. This category measures whether or not all employees have received the annual training, but it does not measure the quality, content, or effectiveness of the training. Other FISMA grading categories have similar gaps. Refining and improving metrics will help achieve better results.

The annual reviews and grades do provide some sense of readiness and security understanding. But, as the Government Accountability Office (GAO) has acknowledged in recent testimony and reports, the FISMA grades do not necessarily reflect an agency's ability to prevent or mitigate the impact of emerging or targeted attacks. We look forward to working with Congress and the Administration to update and improve upon FISMA and its continued, evolving implementation.

IT Vendor Roles and Responsibilities

As providers of information systems and security solutions to the federal agencies, our members take their responsibilities in FISMA compliance and effective information security seriously. Companies, in the course of their product and service development, also have a responsibility to incorporate the latest and greatest technology security tools and best practices. In addition, industry continues its efforts with the National Institute of Standards and Technology (NIST) to help drive effective standards and guidance to the agencies on information security practices.

In turn, government agencies should be encouraged to consider new technologies, best practices, and appropriate standards requirements that do not curtail their ability to take advantage of industry advances. In one example, many companies are moving toward the software-as-a-service model for their data management services. FISMA and OMB's implementing guidance do not explicitly prohibit software-as-a-service or other emerging technology options, but we have seen that government agencies tend to discount this technology due to preconceived and possibly misinformed notions about security. Given that new Internet technology has the potential to dramatically enhance government performance at a substantially lower cost, FISMA should affirm that government agencies consider such emerging technologies and conduct an objective assessment of their security, rather than reject them simply because they are new. If implemented appropriately, they can certainly be part of secure solutions. Federal agencies should not fall behind the curve by limiting their procurement options because preconceived compliance concerns prevent efforts to achieve greater efficiencies, better service, and improved security.

As part of an overall public-private-partnership, government and industry also need to find ways to effectively share information that enables a more robust and mutual understanding of the challenges we are facing so that we can collaborate and work together toward solutions to address those challenges.

Recommendations for Updates and Improvements

There are six areas of FISMA and federal agency information security that we have identified for updates and improvements. The adjustments may be in the law itself in some cases, and in implementing guidance or agency policies and procedures in other cases. We are happy to work with you and our partners in OMB and the agencies to help determine the best approach for each.

Reform Annual Agency Information Security Program Approval Process

On an annual basis, OMB must approve or disapprove federal agency information security plans and programs and ensure they are sufficient to provide information security for the information and information systems that support the operations and assets of the agency. These include a wide range of operations provided or managed by another agency, contractor, or other source.[3] We recommend that this review process be re-evaluated and strengthened to ensure that the agency programs not only have sufficient paper plans but also have validated processes and resources in place to execute those plans.

In reality, the disparity among agency information security programs and policies can create confusion when it comes time to contract for services. For example, Section 3544 outlines Federal Agency Responsibilities for the head of the agency, which includes "...information collected or maintained by or on behalf of the agency."[4] While the language in the law seems clear about the agency head responsibilities, including those services provided by contractors, it is not always clear in practice. We believe that clarification and harmonization of contractor

[3] See Appendix B.
[4] Federal Information Security Management Act, Title III of the E-Government Act of 2002 (P.L. 107-347).

roles and responsibilities related to supporting FISMA requirements – could improve consistency among contracts and improve government security among the agencies.

Remove Barriers to Innovation

Second, while the FISMA statute acknowledges the advanced, dynamic, robust, and effective market solutions that industry can bring to bear, the compliance checklists used by the agencies do not account for innovative market developments and solutions. Technology advancements can provide increased efficiencies and productivity as well as security. FISMA should not be used as a market barrier for these new offerings when the providers can demonstrate that they meet the requirements.

Increase Accountability

Third, it has been more than 10 years since the Clinger-Cohen Act amended the Paperwork Reduction Act and created the CIO position for federal agencies and established capital planning and investment control and performance and results-based management.[5] In 2004, GAO reported on the evolution of the CIO's role and recommended that Congress further investigate the need to reform or modernize the role of the CIO. We believe that in addition to modernizing the role of the CIO, federal Chief Information Security Officer (CISO) positions need to be studied and rationalized to ensure that both the CIO and the CISO are organized, authorized, and funded to ensure that the agency head maintains the accountability that FISMA requires. For example, an agency CIO may not have clear budget or operating authority. Additionally, the CISO most often does not have sufficient authority or integration into the senior management of an agency. If we look at the private sector, we can see some clues about how to address this concern. We are seeing an evolution toward a more active CISO in the senior management structure of an organization and more fully engaged in the risk management and security decisions of the corporation.

This is a paradigm that should be reflected in the organization of every agency's senior management ranks. Homeland Security Presidential Directives 7 and 12 (HSPD-7 and HSPD-12) both reinforce the need to bring the key components of security leadership in the organization together to address security strategies in a cohesive, integrated manner by addressing the need to bring the cyber, physical, and personnel components of the risk spectrum together. A strengthened FISMA could help to break down current silos and make coordinated management decisions that can more fully permeate the organization. We need to give flexibility to agencies to determine how best the information security component fits into their operations, while bringing the function into a senior management role and, ideally, providing the commensurate budgetary and resources authority to that function and its obligations. From the private sector perspective, it appears that FISMA is not being effectively reinforced through the authorization and appropriations process, and we think that connection could make a significant improvement in the implementation of FISMA requirements and information security programs. ITAA believes that the agencies, OMB, the authorizers, and the appropriators could more closely

[5] P.L. 104-106 February 10, 1996. The law, initially entitled the Information Technology Management Reform Act (FIMRA), was subsequently renamed the Clinger-Cohen Act in P.L. 104-208, September 30, 1996.

coordinate their approaches to information security to ensure that effective investments are proposed and made, with appropriate consequences for inaction.

Enhance Federal Cyber Risk Management

Fourth, a greater understanding of the threat to the information security of the federal agencies is a key element to an improved risk management approach. Today, some federal agencies are operating in the dark. They have not incorporated unclassified information into a risk assessment, and they do not have adequate access to classified briefings, or the classified communications capabilities necessary to receive sensitive information on a timely basis. We were pleased to learn that the CIO Council did receive a classified briefing after the recent cyber attacks in Estonia, but once again, that information was provided after the fact rather than in real-time.

An updated FISMA should articulate the need for at least an annual federal government information security risk assessment incorporating required assessments by the federal agencies. Those assessments should encompass both unclassified and classified information and should also include input from the private sector, as many companies have deep insight into network activity, the overall health of the Internet, and the constantly evolving threats to agencies, businesses, and individuals in cyberspace. That requirement would compel the agencies to identify relevant staffing and resource needs and, as a result, better understand how to mitigate the most urgent risks.

We also need to embrace a true risk management approach. We know we cannot achieve perfect security – for either information or physical assets. Therefore, the decisions that agencies make need to reflect risk assessments that prioritize the threats based on the potential consequences of inaction. This will compel more rigor in the risk assessment process in the agencies, encourage preventative measures rather than merely reactive measures, and thereby improve the federal government's overall readiness.

Harmonize and Enhance Audit and Oversight Methods

Fifth, the diversity in the agencies' grades, compliance levels, and information security practices reflects the diversity in the audit processes and capabilities in the agencies and in GAO. There are two ways to remedy that discrepancy and reflect improvements and remaining gaps in information security practices as a result. First, we should be able to attain a more consistent methodology for the IGs' examinations upon which the FISMA compliance is assessed, as today the IGs in the agencies do not have a common examination approach. Second, we can undertake efforts to build the capacity of the IG and GAO auditors through additional resources and training. For example, NIST could conduct training for auditors that leverages the good guidance that they have provided on FISMA and gives more clarity and confidence that the assessments are measuring effectiveness and improvements in information security.

Expand Federal Cyber Response Capabilities

Sixth and finally, we believe there is an operational component that FISMA can directly address going forward. FISMA requires OMB to maintain the operation of a central federal information security incident center. FISMA was in development prior to the passage of the Homeland Security Act, so it did not delineate the role of the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) in supporting OMB for that function, which it does today. Given the timing of FISMA's initial enactment as part of the Homeland Security Act and subsequent replacement in the current version in the E-Government Act, we need a thoughtful review. Specifically, FISMA should be updated to reflect the existence of the US-CERT and to clarify its role and responsibilities. As such, more attention should be paid to the resources needed for US-CERT to perform its government-wide function for FISMA as well as to maintain its national mission described in the Homeland Security Act and critical infrastructure protection requirements outlined in HSPD-7. While FISMA reflects a strategic approach over time, it can also help improve the day-to-day operations of the very response center upon which the agencies rely.

As we are looking at the future of FISMA, I would also like to take an even broader view regarding the operational component of our overall information security needs. Information security is a large part of resiliency, business continuity, continuity of government, and emergency functions. We should take the opportunity to integrate the information security component of FISMA with interagency incident management functions such as the DHS National Communications System (NCS) and Emergency Service Function 2 for Communications (ESF-2), the National Incident Management System (NIMS), and the National Response Plan (NRP).

Conclusion

In closing, we commend the committee for highlighting the importance of information security and for examining how we can improve FISMA and federal agency IT security practices going forward. FISMA can be strengthened if we establish processes and metrics that truly measure information security and help guide investments in personnel, capabilities, and technical controls that can more fully document the true security state of complex federal computing enterprises. We need to get beyond counting on compliance; we need to embrace the public-private partnership that information security requires; and we need to take steps that improve both the policy and the practice of IT security. We appreciate the invitation to share our thoughts and recommendations, and we stand ready to engage with Congress and our government partners going forward.

Appendix A

New York Times
May 29, 2007
Digital Fears Emerge After Data Siege in Estonia

By MARK LANDLER and JOHN MARKOFF

TALLINN, Estonia, May 24 — When Estonian authorities began removing a bronze statue of a World War II-era Soviet soldier from a park in this bustling Baltic seaport last month, they expected violent street protests by Estonians of Russian descent.

They also knew from experience that "if there are fights on the street, there are going to be fights on the Internet," said Hillar Aarelaid, the director of Estonia's Computer Emergency Response Team. After all, for people here the Internet is almost as vital as running water; it is used routinely to vote, file their taxes, and, with their cellphones, to shop or pay for parking.

What followed was what some here describe as the first war in cyberspace, a monthlong campaign that has forced Estonian authorities to defend their pint-size Baltic nation from a data flood that they say was set off by orders from Russia or ethnic Russian sources in retaliation for the removal of the statue.

The Estonians assert that an Internet address involved in the attacks belonged to an official who works in the administration of Russia's president, Vladimir V. Putin.

The Russian government has denied any involvement in the attacks, which came close to shutting down the country's digital infrastructure, clogging the Web sites of the president, the prime minister, Parliament and other government agencies, staggering Estonia's biggest bank and overwhelming the sites of several daily newspapers.

"It turned out to be a national security situation," Estonia's defense minister, Jaak Aaviksoo, said in an interview. "It can effectively be compared to when your ports are shut to the sea."

Computer security experts from NATO, the European Union, the United States and Israel have since converged on Tallinn to offer help and to learn what they can about cyberwar in the digital age.

"This may well turn out to be a watershed in terms of widespread awareness of the vulnerability of modern society," said Linton Wells II, the principal deputy assistant secretary of defense for networks and information integration at the Pentagon. "It has gotten the attention of a lot of people."

The authorities anticipated there would be a backlash to the removal of the statue, which had become a rallying point for Estonia's large Russian-speaking minority, particularly as it was removed to a less accessible military graveyard.

When the first digital intruders slipped into Estonian cyberspace at 10 p.m. on April 26, Mr. Aarelaid figured he was ready. He had erected firewalls around government Web sites, set up extra computer servers and put his staff on call for a busy week.

By April 29, Tallinn's streets were calm again after two nights of riots caused by the statue's removal, but Estonia's electronic Maginot Line was crumbling. In one of the first strikes, a flood of junk messages was thrown at the e-mail server of the Parliament, shutting it down. In another, hackers broke into the Web site of the Reform Party, posting a fake letter of apology from the prime minister, Andrus Ansip, for ordering the removal of the highly symbolic statue.

At that point, Mr. Aarelaid, a former police officer, gathered security experts from Estonia's Internet service providers, banks, government agencies and the police. He also drew on contacts in Finland, Germany, Slovenia and other countries to help him track down and block suspicious Internet addresses and halt traffic from computers as far away as Peru and China.

The bulk of the cyberassaults used a technique known as a distributed denial-of-service attack. By bombarding the country's Web sites with data, attackers can clog not only the country's servers, but also its routers and switches, the specialized devices that direct traffic on the network.

To magnify the assault, the hackers infiltrated computers around the world with software known as bots, and banded them together in networks to perform these incursions. The computers become unwitting foot soldiers, or "zombies," in a cyberattack.

In one case, the attackers sent a single huge burst of data to measure the capacity of the network. Then, hours later, data from multiple sources flowed into the system, rapidly reaching the upper limit of the routers and switches.

By the end of the first week, the Estonians, with the help of authorities in other countries, had become reasonably adept at filtering out malicious data. Still, Mr. Aarelaid knew the worst was yet to come. May 9 was Victory Day, the Russian holiday that marks the Soviet Union's defeat of Nazi Germany and honors fallen Red Army soldiers. The Internet was rife with plans to mark the occasion by taking down Estonia's network.

Mr. Aarelaid huddled with security chiefs at the banks, urging them to keep their services running. He was also under orders to protect an important government briefing site. Other sites, like that of the Estonian president, were sacrificed as low priorities.

The attackers used a giant network of bots — perhaps as many as one million computers in places as far away as the United States and Vietnam — to amplify the impact of their assault. In a sign of their financial resources, there is evidence that they rented time on other so-called botnets.

"When you combine very, very large packets of information with thousands of machines, you've got the recipe for very damaging denial-of-service attacks," said Jose Nazario, an expert on bots at Arbor Networks, an Internet security firm in Ann Arbor, Mich.

In the early hours of May 9, traffic spiked to thousands of times the normal flow. May 10 was heavier still, forcing Estonia's biggest bank to shut down its online service for more than an hour. Even now, the bank, Hansabank, is under assault and continues to block access to 300 suspect Internet addresses. It has had losses of at least $1 million.

Finally, on the afternoon of May 10, the attackers' time on the rented servers expired, and the botnet attacks fell off abruptly.

All told, Arbor Networks measured dozens of attacks. The 10 largest assaults blasted streams of 90 megabits of data a second at Estonia's networks, lasting up to 10 hours each. That is a data load equivalent to downloading the entire Windows XP operating system every six seconds for 10 hours.

"Hillar and his guys are good," said Bill Woodcock, an American Internet security expert who was also on hand to observe the response. "There aren't a lot of other countries that could combat that on his level of calm professionalism."

Estonia's defense was not flawless. To block hostile data, it had to close off large parts of its network to people outside the country.

"It is really a shame that an Estonian businessman traveling abroad does not have access to his bank account," said Linnar Viik, a computer science professor and leader in Estonia's high-tech industry. "For members of the Estonian Parliament, it meant four days without e-mail."

Still, Mr. Viik said the episode would serve as a learning experience. The use of botnets, for example, illustrates how a cyberattack on a single country can ensnare many other countries.

In recent years, cyberattacks have been associated with Middle East and Serbian-Croatian conflicts. But computer systems at the Pentagon, NASA, universities and research labs have been compromised in the past.

Scientists and researchers convened by the National Academy of Sciences this year heard testimony from military strategy experts indicating that both China and Russia have offensive information-warfare programs. The United States is also said to have begun a cyberwarfare effort.

Though Estonia cannot be sure of the attackers' identities, their plans were posted on the Internet even before the attack began. On Russian-language forums and chat groups, the investigators found detailed instructions on how to send disruptive messages, and which Estonian Web sites to use as targets.

"We were watching them being set up in real time," said Mr. Aarelaid, who weeks later could find several examples using Google.

For NATO, the attack may lead to a discussion of whether it needs to modify its commitment to collective defense, enshrined in Article V of the North Atlantic Treaty. Mr. Aarelaid said NATO's Internet security experts said little but took copious notes during their visit.

Because of the murkiness of the Internet — where attackers can mask their identities by using the Internet addresses of others, or remotely program distant computers to send data without their owners even knowing it — several experts said that the attackers would probably never be caught. American government officials said that the nature of the attacks suggested they were initiated by "hacktivists," technical experts who act independently from governments.

"At the present time, we are not able to prove direct state links," Mr. Aaviksoo, Estonia's defense minister, said. "All we can say is that a server in our president's office got a query from an I.P. address in the Russian administration," he added, using the abbreviation for Internet protocol. Moscow had offered no help in tracking down people who the Estonian government believes may be involved.

A spokesman for the Kremlin, Dmitri S. Peskov, denied Russian state involvement in the attacks and added, "The Estonia side has to be extremely careful when making accusations."

The police here arrested and then released a 19-year-old Estonian man of Russian descent whom they suspected of helping to organize the attacks. Meanwhile, Estonia's foreign ministry has circulated a document that lists several Internet addresses inside the Russian government that it said took part in the attacks.

"I don't think it was Russia, but who can tell?" said Gadi Evron, a computer security expert from Israel who spent four days in Tallinn writing a post-mortem on the response for the Estonians. "The Internet is perfect for plausible deniability."

Mr. Evron, an executive at an Internet security firm called Beyond Security, is a veteran of this kind of warfare. He set up the Computer Emergency Response Team, or CERT, in Israel. Web sites in Israel are regularly subjected to attacks by Palestinians or others sympathetic to their cause.

"Whenever there is political tension, there is a cyber aftermath," Mr. Evron said, noting that sites in Denmark became targets after a newspaper there published satirical cartoons depicting the prophet Muhammad.

The attacks on Estonia's systems are not over, but they have dropped in volume and intensity, and are aimed mainly at banks. The last major wave of attacks was on May 18.

Now that the onslaught has ebbed, Mr. Aarelaid is mopping up. A few days ago, he managed to get to the sauna with Jaan Priisalu, the head of computer security at Hansabank, and other friends from Estonia's Internet security fraternity.

"I'm a simple I.T. guy," he said, gazing at a flickering computer screen. "I know a lot about bits and packets of data; I don't know about the bigger questions. But somebody orchestrated this thing."

Mark Landler reported from Tallinn and John Markoff from San Francisco. Steven Lee Myers contributed reporting from Moscow.

Appendix B

FISMA
Section 3544. Federal Agency Responsibilities

"(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3543(a)(5), to 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, that includes—

"(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

"(2) policies and procedures that—

"(A) are based on the risk assessments required by paragraph (1);

"(B) cost-effectively reduce information security risks to an acceptable level;

"(C) ensure that information security is addressed throughout the lifecycle of each agency information system; and

"(D) ensure compliance with—

"(i) the requirements of this subchapter;

"(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;

"(iii) minimally acceptable system configuration requirements, as determined by the agency; and

"(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

"(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

"(4) security awareness training to inform personnel, including contractors and other users of information systems

that support the operations and assets of the agency, of—

"(A) information security risks associated with their activities; and

"(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

"(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing—

"(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and

"(B) may include testing relied on in a evaluation under section 3545;

"(6) 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;

"(7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including—

"(A) mitigating risks associated with such incidents before substantial damage is done;

"(B) notifying and consulting with the Federal information security incident center referred to in section 3546; and

"(C) notifying and consulting with, as appropriate—

"(i) law enforcement agencies and relevant Offices of Inspector General;

"(ii) an office designated by the President for any incident involving a national security system; and

"(iii) any other agency or office, in accordance with law or as directed by the President; and

"(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Mr. CLAY. Thank you so much for that testimony.

Mr. Kurtz, you may proceed.

STATEMENT OF PAUL KURTZ

Mr. KURTZ. Thank you, Chairman Clay. It is a pleasure to be here today. Thank you for the invitation.

I am here today to talk about how certain information and security developments in the private sector will impact the future of FISMA and follow-on information security, guidance, and controls.

As a start, I would note FISMA is a good step, a good first step, and a good foundation; however, current law and supporting implementation guidance must evolve if it is to be effective in light of new technology and continually emerging threats.

My testimony today is divided into two parts: strengths and weaknesses associated with FISMA, as well as discussing changes in the private sector and how those will influence the evolution of FISMA and other Federal IT security measures in the coming year.

First of all, the state of FISMA. Although there are flaws in its implementation, I would argue that the overall impact of FISMA has been positive.

The strengths, transparencies: agencies must now show how their overall information security strategy and budget fit into the general mission and goals of an agency.

Second, accountability: agencies must report on their progress toward improving information security by at least categorizing data based on risk and certifying systems. They also must test security controls and contingency plans and they must assign risk impact levels. Of course, now we have standards that have been put together by NIST, like 800–53, which at least establish a baseline.

However, there are weaknesses. One, FISMA and supporting guidance do not provide an enterprise-wide assessment of risk. What is the overall risk associated with a given agent's IT security system? We have misleading scores. The scores measure not only whether agencies pursue compliance processes, but not whether IT systems are actually secure. In other words, there is perhaps a false sense of security associated with the scores.

A lack of consequences for non-compliance: FISMA has no real enforcement capability outside of OMB being able to threaten to move money around.

The inability to adapt to emerging technologies: in other words, we have new technologies that Mr. Bond has talked about that FISMA can't handle so well.

Many of these concerns I would argue can be addressed by improving FISMA implementation guidance and do not necessarily require a change in the law; however, both committees' oversight and looking for reporting would be extremely helpful.

There have been several developments in the private sector which I think should be highlighted here today.

First of all, the private sector is empowering CIOs and CISOs. Mr. Bond talked about that. That is a very important development. But there is also the changing nature of IT. This is an incredibly important issue. We have a shifting paradigm from a client server environment where all of the applications are loaded on your computer, to one where we are building or using software and data

that is stored offsite via the Internet. This is sometimes referred to as Web 2.0.

Currently, FISMA guidance is skewed toward the client server environment, which means that some of the great efficiencies that are available through such things as software as a service are being passed by by the Federal Government because of perceived issues associated with FISMA compliance. Guidance needs to be updated sooner rather than later, as Mr. Bond has talked about, to ensure that agencies can take advantage of software as a service.

Right now I can name several cases where agencies are, if you will, in a holding pattern because they don't think software as a service is going to work.

Finally, I want to highlight the need to evolve to a more common international information security standard. FISMA is, if you will, the Government information security standard, and it is good, it is solid; but meanwhile the private sector is evolving toward a new standard, ISO 27001, which sounds a little technical but agencies and firms around the world are moving to this new standard. It would be good if FISMA could at least have some level of agreement with what is happening in the 27001 world. In other words, if I am compliant with 27001, this new revised standard, I can be deemed in compliance with FISMA. This would bring great efficiency to Federal agencies and reduce the cost for taxpayers, as well.

I will conclude my remarks there.

[The prepared statement of Mr. Kurtz follows:]

GOOD HARBOR
CONSULTING, LLC

Prepared Testimony of
Paul B. Kurtz
Chief Operating Officer
Good Harbor Consulting

Before the Subcommittee on Government Management, Organization, and Procurement and the Subcommittee on Information Policy, Census, and National Archives of the House Committee on Oversight and Government Reform

"Federal IT Security: The Future of FISMA"

Room 2154, Rayburn House Office Building
Thursday, June 7, 2007
2:00PM

4100 N. Fairfax Drive • 3rd Floor, Suite 301 • Arlington, VA 22203-1629
Tel. 703.812.9199 • www.goodharbor.net

Introduction

Chairman Towns, Chairman Clay, Congressman Bilbray, Congressman Turner and Members of the Oversight and Government Reform Committee, thank you for the opportunity to testify today. My name is Paul Kurtz, and I am the Chief Operating Officer and Director of the Information Technology Security Practice at Good Harbor Consulting, LLC.

Good Harbor Consulting, LLC provides strategic advice and counsel for a broad range of clients – including Fortune 500 companies, industry associations, systems integrators, and innovative technology start-ups – in the areas of homeland security, cyber security, critical infrastructure protection and counterterrorism. Our IT security consulting practice provides clients with leading-edge strategies and solutions for a wide range of IT security challenges. My comments today are personal and do not necessarily represent the views of Good Harbor Consulting or its clients.

Before joining Good Harbor Consulting, I was the Executive Director of the Cyber Security Industry Alliance (CSIA), which is the only advocacy group dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. Previously, I served at the White House on the National Security Council and Homeland Security Council. On the NSC, I served as Director of Counterterrorism and Senior Director of the Office of Cyberspace Security. On the HSC, I was Special Assistant to the President and Senior Director for Critical Infrastructure Protection.

I am here today to talk about how certain information security developments in the private sector may have an impact on the future of the Federal Information Security Management Act (FISMA) and follow-on information security regulations and controls. FISMA is a good first step in what will surely be a long – and increasingly collaborative – process between the public and private sectors in safeguarding the integrity of the Federal IT infrastructure. However, as timely and well-intentioned as FISMA was in 2002, the current law must evolve if it is to be effective in light of new technology and continually emerging threats.

First, I will address the strengths and weaknesses of FISMA as it is currently implemented. Second, I will discuss how changes in the private sector will influence the evolution of FISMA and other federal IT security measure in coming years. Three specific trends are:

- The need for greater empowerment of federal Chief Information (Security) Officers
- The changing nature of IT and information security
- The global drive towards common security standards

The State of FISMA

As you are aware, the effectiveness of FISMA is widely debated. Although there are flaws in its implementation, I would argue that the overall impact of FISMA has been positive. Even FISMA's biggest critics acknowledge that this initiative has the potential of being a powerful mechanism for improving information security throughout the federal government. This section briefly discusses the act's strengths and weaknesses in order to set the stage for how private-sector developments may influence FISMA's evolution.

Strengths

FISMA has served as an important management and assessment tool for federal agency IT systems. This effort has brought renewed emphasis to government-wide information security:

- **Transparency:** In order to be in accordance with FISMA, agencies must show how their overall information security strategy and budget fit in with the general mission and goals of the agency.

- **Accountability:** FISMA requires federal agencies to report to the Office of Management and Budget (OMB) and to Congress on their progress toward improving information security by certifying and accrediting systems, testing security controls and contingency plans, and assigning risk impact levels. Furthermore, the resulting report cards issued by Congress raise visibility of IT vulnerabilities and expose government agencies to public scrutiny.

- **Standardization:** The National Institute for Standards and Technology (NIST) has issued several strong standards – notably *Special Program 800-53: Recommended Security Controls for Federal Information Systems* – and tools such as the [PRISMA] database to help determine the extent to which IT systems across agencies need to be secured.

Personally, I recall my experience at the White House in 2000, when we had very little insight into the state of IT security across Federal agencies. We had no common standards in place and no data on how much agencies were spending to address security. We have certainly come a very long way in seven years thanks to the Government Information Security Reform Act (GISRA) and FISMA.

Weaknesses

Despite the near-universal participation of government agencies in the FISMA reporting process, many observers suggest that there hasn't been an appreciable increase in Federal IT security in the past five years. Possible reasons for this include:

- **Misleading scores:** FISMA does not necessarily address whether cyber security has been improved in an agency. Rather, the act as currently implemented measures only whether agencies pursue processes for assessing, testing, and managing IT security. For example, agencies that simply complete dozens or hundreds of certification and accreditation reports can earn high scores even if their systems do not pass the required tests or are not subsequently hardened and monitored. Moreover, evaluation standards and techniques (especially if implemented by contractors) vary across agencies.

- **Narrow metrics:** Conversely, FISMA as currently implemented does not always accurately document or measure successful agency efforts to secure their information systems. As Interior Department CIO Hord Tipton noted last year, ""We fended off four billion probes, scans, attacks [in 2005] without any significant breaches. It doesn't show up in the FISMA report." For this reason, many critics argue that a "one size fits all" approach to security does not make sense across different agencies,

- **Lack of consequences for non-compliance:** Over the past five years, three of the largest departments of the federal government – State, Defense, and Homeland Security – have received low grades from Congress on their FISMA compliance. As the Government Accountability Office concluded in 2006, many "federal agencies have not adequately designed and effectively implemented policies for periodically testing and evaluating information security controls." Outside of OMB's limited ability to redirect agency spending, there is no enforcement mechanism or incentive structure in place to ensure that failing departments take the necessary steps to improve IT security.

- **Inability to adapt to emerging technologies:** The implementation of FISMA security controls often betrays a bias against the adoption of new and emerging technologies. Despite the rise of software-as-a-service (which is later discussed in more detail) and mobile technologies in recent years, FISMA guidance and NIST security controls have not expanded accordingly. Since Federal security controls do not reference third-party internet-accessible software and data-on-demand business models, some agencies are quick to reject these solutions as non-compliant, even though they offer robust levels of security. This creates a "catch-22" situation. Federal agencies have no incentive to invest in new technologies since they cannot successfully be brought into FISMA compliance. At the same time, NIST will not adapt its security controls to new technologies because a critical mass of users does not exist within the public sector.

This in turn leads to increased inefficiencies and ultimately less security with respect to federal IT systems.

- **Failure to address telecommunications continuity of operations:** Finally, FISMA does not require Federal agencies to establish and regularly test continuity of operations for telecommunications services. Section 3544 (8) addresses continuity of IT systems, but does not explicitly address telecommunications. As convergence continues, it will be very important to ensure rigorous communication COOP programs are in place.

Many of these concerns can be addressed by improving FISMA implementation guidance without necessarily requiring a change in law.

The Private Sector

Several recent developments demonstrate the need to change how the federal government thinks about information security. FISMA may have been created in part to help government agencies lead by example when it comes to IT security, but the private sector has shown that still more needs to be done. As the IT security landscape continues to expand, the federal government must anticipate, react, and adapt to these new developments in order to create stronger and more effective ways to safeguard our Federal IT infrastructure.

Empowering the Chief Information Security Officer

Chief Information (and Security) Officers (CIO/CISO) in both the public and private sectors have traditionally been responsible for IT security within their respective organizations but rarely given the authority to effectively enforce security protocols. However, this attitude towards securing information systems seems to be changing in the private sector. While it used to be difficult to rationalize the return on investment on increased security precautions, the proliferation of worms, viruses, Trojan horses and the individuals who spread them has sparked an interest in safeguarding IT systems and networks from malicious attacks.

Several corporations have recognized the need of integrating the Chief Information Security Officer (CISO) at the highest executive levels (in some case reporting directly to chief financial and executive officers) and empowering the CISO with expansive powers and responsibilities that range from incident response to IT compliance to customer data privacy. Moreover, many CISOs are brought in as risk managers, rather than simply IT practitioners, which grants them more influence in long-term strategic planning.

There are indications that the federal government is drawing lessons from these trends. The House Committee on Veterans' Affairs, for instance, acknowledges that it was the lack of CIO and CISO authority that contributed to the May 2006 theft of an employee laptop, which housed confidential data. To that end, I commend legislation by Congressman Buyer to empower the Veterans Affairs Department's CIO to enforce information security in the VA IT department and to create new high-level information security positions within the agency. Such initiatives should be further strengthened and replicated in other agencies across the federal government. For example, CISOs should also have the latitude to approve budgets and work on projects they perceive as critical to the agency's information security rather than simply having to fulfill the certification and accreditation requirements posed by FISMA.

The Changing Nature of IT

In addition to the changing role of the CISO, the IT environment itself is undergoing a transformation. Historically, the federal government has relied on the client-server model, where IT systems procured from vendors are then implemented, maintained, and upgraded in-house.

Trends in the private sector, however, suggest a major paradigm shift. Many companies are migrating towards internet accessible software and data services, which are often referred to as "software-as-a-service" (SAAS). Software as a Service consists of applications and databases that are delivered to customers over the internet from a shared IT infrastructure. By applying economies of scale to the development and operation of these applications, a SAAS provider can offer better, cheaper, more reliable applications than companies can provide themselves. Tens of thousands of businesses, including large financial enterprises, have already migrated sensitive data to SAAS providers and data warehouses, and it is projected that SAAS will account for nearly half of all software sales in the private sector within the next five years.

Although federal agencies have been slow to adopt SAAS, I am confident that this migration to software and data services will eventually occur in the public sector as the government begins to recognize the cost savings and performance advantages of SAAS. This Committee should make sure that FISMA facilitates this evolution rather than hinders it.

Global Drive to Common Standards

Given the changing nature of the IT landscape, information security legislation needs to adapt accordingly. Guidance from OMB and NIST has been adequate in addressing the client-server paradigm, but standards should be adjusted to govern the eventual migration by the public sector to SAAS platforms.

One option is to begin more closely aligning FISMA with recently updated international cyber standards. The International Organization of Standardization has issued a revised cyber security standard – ISO 27001 – that can be applied towards commercial enterprises and non-profit organizations as well as government agencies. IS0 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an information security management system within the context of the organization's overall risk management processes. ISO 27001 is comprehensive, covering security policy, internal organization, asset management, human resources, physical and environmental security, communications and operations management, access control, acquisition, incident, and continuity management. In addition, ISO 27001 provides for third-party certification of an entity's security. However, unlike the comparably rigid standards set by OMB and NIST, ISO 27001 can be customized to the needs of individual organizations, thereby avoiding FISMA's "one size fits all" approach to cyber security.

This is not to suggest that the standards established by OMB and NIST should be disregarded altogether. In fact, NIST guidance is quite good. However, we must move toward a common global information security standard. The US government could lead the drive toward a common standard for the public and private sectors by accepting ISO 27001 as an equal to FISMA. In addition, acceptance of ISO 27001 certification would also improve transparency of Federal information security and reduce the bureaucracy and costs associated with current FISMA compliance procedures.

Conclusion

Thank you for the opportunity to testify on these issues today. As I close my testimony, I want to emphasize the fact that FISMA has played a salient role in raising awareness of IT security issues and demonstrably improved information security throughout the federal government. When I was still working at the White House in 2001, no common standards existed. FISMA was the first legislation that took information security seriously, and – despite its flaws – it has served us well.

However, for the reasons I have cited, there is still much more to be done to effectively safeguard federal information security. With that, I am pleased answer any questions you may have.

Mr. CLAY. Thank you so much, Mr. Kurtz, for those suggestions. Mr. Carlson, you may proceed.

STATEMENT OF JOHN W. CARLSON

Mr. CARLSON. Great. Thank you. Thank you for the opportunity to testify on information security practices within the financial services industry and how they may be of use to the Federal agencies in meeting the goals of FISMA.

I am John Carlson. I am the executive director of BITS. We are a division of the Financial Services Roundtable focusing on technology and operations issues to promote best practices in a strong national financial infrastructure.

I would like to briefly highlight the risk and threat environment faced by financial institutions today and our efforts, which could be applied to strengthen the Federal Government's information security programs.

The cyber security threat environment is constantly evolving, and some risks are increasing. Phishing, cyber squatting, viruses, worms, and other forms of attack are endemic. Hackers are closing the window between the discovery of a software flaw and the exploitation of that flaw. Criminals are using social engineering to trick consumers into providing personal information that can facilitate fraud and identity theft. Highly publicized breaches, both public and private sector, end the resulting loss of the theft of personally identifiable information do undermine consumer confidence, and that leads to concern about identity theft, which remains high.

In response to these threats, our members companies are constantly thinking about these risks and have developed numerous guides and other forms of collaboration to mitigate them. We have developed tools to secure better data, to respond more effectively to data breaches. For example, we developed a guide in conjunction with the American Bankers Association to help financial institutions respond to data breaches, which is in harmony, by the way, with the Graham-Leach-Bliley Act's information security safeguards rule, which provides a very helpful foundation for the financial services industry.

In addition, we work with our member companies to respond to high-profile breaches, such as the TJX Company's breach several months ago.

We have engaged also major software companies by outlining our sector's high security needs, even providing a lab to test software products against baseline security requirements and developing a practitioner's guide for patching software for complex information technology environments, in many cases very similar to Government in terms of the complexity and legacy systems.

We have also developed a number of consumer education materials that help consumers secure their computers and avoid the lure of fraudsters.

We have also looked at successful factors for security and awareness programs which financial institutions are required to provide to their employees, like Government agencies, as well.

Efforts to make e-mail more secure and reliable could be helpful in reducing the amount of spam and malicious software that is transmitted through e-mail. We released a tool kit several months

ago that recommends financial institutions and others adopt specific protocols designed to improve e-mail security. We think if Government adopted those we would go a long way in addressing some of the e-mail-related problems we are dealing with today.

Our work in overseeing third-party surveillance providers could be helpful to Government agencies in procuring services and overseeing vendors. For example, the Financial Institutions Shared Assessments Program, which we launched in 2006, streamlines the service provider risk assessment process while raising the bar on security. We currently have 50 financial institutions, service providers, and assessment firms that are involved in this program.

We are also looking presently at the issue of wireless technologies and some of the security risks that may result from those technologies, and assuring that we are addressing those risks adequately.

We have also outlined a number of research and development funding priorities that we think, if the Government adopted, would be very helpful for our sector. These would include areas such as better Internet protocols, better enrollment and identity credential management, better understanding of insider fraud and threats, and better ways of measuring the return on investment of security technology.

And perhaps most important to Congress is our work to assist victims of identity theft while at the same time helping law enforcement agencies investigate and prosecute identity theft crimes. The Identity Theft Assistance Center, another division of the Roundtable which BITS helped to establish several years ago, provides a free victim assistance service to customers of our member companies. Since it opened in 2004, it has helped 16,000 consumers restore their financial identity. Also, data supplied by ITAC with the consent of consumers is helping catch the individuals who commit these crimes.

The financial service sector was the first sector to establish an Information Sharing and Analysis Center in the late 1990's, which continues to be a model for successful information sharing on cyber and physical threats. In addition, our sector established a Coordinating Council shortly after 9/11 to provide a means of collaborating across the sector, with other sectors, and with the Departments of Homeland Security, Treasury Department, and others.

Before I conclude, I want to remind the committee that financial institutions are heavily regulated and constantly supervised. Our financial regulators have issued numerous regulations and supervisory guidance on information security, with the Graham-Leach-Bliley safeguards rule as an important foundation. Efforts by regulatory agencies have had a positive impact on improving information security through a risk-based approach, which is very important.

Government can help the industry and society in a number of ways in dealing with the threats we are dealing with today. A number that I would like to point out would be: implementing a Social Security verification program to reduce fraud and identity theft; issuing more secure Government credentials; and permitting financial institutions to transmit data to Government agencies like the IRS in encrypted format.

In closing, secured information is an ongoing process that requires constant vigilance, ongoing enhancements to address new and emerging threats, in collaboration with partners. I believe our efforts can be helpful to Government agencies in complying with the goals of FISMA.

Thank you for the opportunity.

[The prepared statement of Mr. Carlson follows:]

112

STATEMENT

OF

JOHN CARLSON
ON BEHALF OF BITS
AND THE FINANCIAL SERVICES ROUNDTABLE

BEFORE THE

UNITED STATES CONGRESS
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
ORGANIZATION, AND PROCUREMENT AND
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND
NATIONAL ARCHIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

HEARING ON
FEDERAL IT SECURITY: THE FUTURE FOR FISMA
JUNE 7, 2007

TESTIMONY OF JOHN CARLSON, EXECUTIVE DIRECTOR, BITS

Introduction

Thank you Chairman Towns and Chairman Clay for the opportunity to submit testimony before your subcommittees about information security best practices within the financial services industry and how these practices may be of use to Federal agencies in meeting the goals of the Federal Information Security Management Act (FISMA).

I am John Carlson, the Executive Director of BITS. BITS focuses on technology and operations issues such as information security, fraud prevention, business continuity and vendor issues where industry cooperation serves the public good. In our ten years, BITS has worked with our member financial institutions, affiliate associations such as the American Bankers Association and Credit Union National Association, government agencies, technology companies, and others to achieve our mission to promote best practices and a strong national financial infrastructure. BITS is a division of The Financial Services Roundtable, a national association that represents 100 of the largest integrated financial services companies providing banking, insurance, investment products, and other financial services to American consumers. Roundtable member companies provide fuel for America's economic engine, accounting directly for $65.8 trillion in managed assets, $1 trillion in revenue, and 2.4 million jobs.

In your invitation letter, you asked me to provide testimony regarding BITS' work and how both the government and private sector can benefit through shared best practices, procurement models, and life-cycle stewardship activities for information technology systems and assets. In my testimony, I will cover three areas. First, I will discuss the risk and threat environment financial institutions currently face and why securing our information technology infrastructure is so important. Second, I will outline some recommendations for the government to strengthen information security programs. Third, I will highlight our efforts to address information security challenges and how these approaches may benefit the government in strengthening information security.

Risk and Threat Environment

Our nation's economic and physical security relies on the security, reliability, recoverability, continuity, and availability of information systems. Information technology security has a direct and profound impact on the government, the private sector, and the nation's critical infrastructure. The financial services sector is an important part of the nation's critical infrastructure. Customer trust in the security and continuity of financial transactions is vital to the stability of the industry and the strength of the nation's economy. The financial sector is a favorite target of cyber criminals as international crime rings, using the Internet for fraud and financial gain, are propagating. The financial sector is also a target for terrorists, as was made clear on 9/11.

The cybersecurity threat environment is constantly evolving and some risks are increasing. Criminals are writing code to compromise systems. Phishing, cybersquatting, viruses, worms, and other forms of attack are endemic.[1] Hackers are closing the window between the discovery of a software flaw and exploitation of that flaw. Criminals are using social engineering to trick consumers into providing personal information that can facilitate fraud and identity theft. Highly-publicized breaches and the resulting loss or theft of personally-identifiable information undermine consumer confidence.

Anxiety about identity theft remains high. However, the combined efforts of the financial services industry, law enforcement, federal financial regulators, and the Federal Trade Commission (FTC), are showing results. For example, The Identity Theft Assistance Center (ITAC), another division of The Roundtable which BITS helped to create, fights identity theft by helping victims recover from this serious crime, partnering with law enforcement to catch and convict criminals, and conducting research on the causes of and solutions to identity theft. The ITAC provides a free victim assistance service to customers of member

[1] Phishing is the use of technology and social engineering to entice consumers to supply personal information such as account numbers, login IDs, passwords, and other verifiable information that can then be exploited for fraudulent purposes, including identity theft. Phishing is most often perpetrated through mass emails and spoofed websites. According to the Anti-Cybersquatting Consumer Protection Act, cybersquatting is registering, trafficking in, or using a domain name with bad-faith intent to profit from the goodwill of a trademark belonging to someone else.

companies. Since it opened in 2004, ITAC has helped 16,000 consumers restore their financial identity. ITAC's research into the experience of actual victims is providing important insight into the causes of identity theft. A recent ITAC survey of 275 victims showed that 42% of identity theft victims knew how the fraud occurred. Of those, the most frequently cited cause was friends, family, and in-home employees

Recommendations for Government

Over the years, BITS members have collaborated to develop numerous guides, toolkits and other publications to identify and address challenges facing the financial services. Many of these efforts may be useful for government agencies in procuring more secure software, sharing information, notifying citizens following a data breach, developing testing/training procedures, managing third party outsourcing, and funding research and development. Most of these documents are publicly available on the BITS website[2].

Financial institutions are heavily regulated and supervised. Financial regulators, primarily through interagency efforts of the Federal Financial Institutions Examination Council (FFIEC), have issued numerous regulations and supervisory guidance on information technology covering many aspects including management, information security, outsourcing, business continuity planning, and consumer protection. Regulators constantly examine financial institutions to ensure compliance with these dynamic requirements. In response, financial institutions continue to demonstrate that they have adequate controls in place to mitigate these risks.

Collectively, these efforts by financial institutions and the financial regulators are helping to improve the resiliency of the financial services industry.

There are several common steps that serve as the foundation for many of our tools that are relevant to government programs:

[2] See www.bitsinfo.org.

- Secure and maintain senior management commitment to ensure that organizations have the appropriate incentives, adequate funding, and training for technicians and users.
- Assess risks on an ongoing basis and participate in information sharing and analysis programs.
- Implement appropriate controls (e.g., access controls, authentication, physical security, encryption, employee background checks, insurance) based on changing risks.
- Manage third party providers effectively and focus on critical interdependencies with other sectors.
- Establish meaningful metrics to measure and understand risks, assess gaps, and measure progress.
- Educate users through training and awareness programs.
- Test regularly to ensure that the technology, people, and processes are working effectively at appropriate levels of assumed residual risk.
- Measure progress through meaningful and independent audits.

Several years ago, BITS outlined seven elements that the Government can pursue to strengthen cybersecurity. We call these seven steps **PREPARE.** The full **PREPARE** statement is included in the Appendix to this testimony, but immediately below are several important elements of these recommendations:

Promote: Government can play an important role in promoting the importance of secure information technology.

Responsibility: Government should promote shared responsibility between suppliers and end users for developing, deploying, and maintaining secure information networks. Government can play an important role in establishing incentives and making producers of software and hardware accountable for the quality of their products.

Educate: Communicate to all users of information technology the importance of safe practices.

Procure: Using its purchasing power and leveraging security requirements and best practices developed by the public and private sectors, government can play an important role in encouraging the information technology industry to deliver and implement more secure systems.

Analyze: Government should collect information and analyze the costs and impact of information security risks, vulnerabilities, and threats and provide this analysis to policy makers.

Research: Government can play an important role in funding research and development in the areas of secure software development practices, testing, and certification programs.

Enforce: Law enforcement must do more to enforce, investigate, and prosecute cyber crimes here and abroad.

During the past year alone, the Federal government has taken several important steps to strengthen cybersecurity, many of which The Roundtable and BITS supported. Examples include:

- Creation and appointment of an Assistant Secretary for Cyber Security and Communications to the Department of Homeland Security (DHS).
- U.S. Senate ratification of the Council of Europe's Convention on Cybercrime, signed by the United States in November 2001.[3]
- Release of the Administration's Identity Theft Task Force Report. The report includes a number of helpful recommendations, including support for a uniform national standard for breach notification, endorsement risk-based approaches and strategies to render lost or stolen data useless by identity thieves, and the

[3] The Convention on Cybercrime is the first and only international, multilateral treaty specifically addressing the need for cooperation in the investigation and prosecution of computer network crimes. It requires global law enforcement cooperation with respect to searches and seizures and provides timely extradition for computer network based crimes covered under the treaty.

recommendation that public and private sectors to limit use of Social Security Numbers (SSNs). The report also appropriately acknowledges the need for financial institutions and law enforcement to use SSNs as identifiers, recommends greater involvement by law enforcement in investigating and prosecuting identity theft crimes, and recommends additional studies. Further, the report includes information on financial services industry efforts to protect data, educate consumers, and assist victims of identity theft and the role of financial regulators in overseeing industry efforts in these areas.

- Completion of the Sector Specific Plans for all of the nation's critical infrastructures, including the Banking and Finance Sector Plan, as part of the Administration's National Infrastructure Protection Plan.
- U.S. Office of Management and Budget requirements for executive departments and agencies to strengthen information security programs.

These are positive steps but much more needs to be done.

Financial Industry Efforts

I want to highlight some examples of the financial services industry's leadership in information security, privacy protection, fraud reduction, vendor management, and identity theft assistance. These efforts are helping the financial services industry mitigate some of the risks it faces.

Members of The Roundtable and BITS are sharing information, analyzing threats, creating best practices, urging the software and technology industries to do more to provide more secure products and services, and combating fraud and identity theft.[4] For example, the financial services industry has established the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) to share information on threats and to coordinate and collaborate with government agencies. The FS-ISAC and the

[4] Many BITS best practices and other deliverables are publicly available on the BITS website (http://www.bitsinfo.org/p_publications.html).

FSSCC continue to work with the U.S. Department of Treasury and DHS to promote information sharing and best practices within the sector and across other critical infrastructure sectors such as telecommunications and energy.

Applying the same **PREPARE** template, let me reference some of financial services industry efforts and how these efforts may benefit the government in strengthening information security.

Promote. As part of an effort to promote secure information technology, financial institutions have developed tools to secure data and respond more effectively to data breaches. The sources of data breaches vary from lost or stolen computers or backup tapes containing sensitive data to insider abuse and hacking. While research by ID Analytics, Inc. indicates that most data compromises do not lead to fraud or identity theft, consumers are understandably concerned about the possible risks posed to their personal and/or account information. Notifying customers of a breach is a complicated and complex process that, if poorly done, can undermine confidence in the financial institution. Care must be exercised in alerting consumers to steps they can take to protect themselves from identity theft and other forms of fraud while averting needless alarm as well as apathy caused by too many false alarms.

The breach involving customers of TJX Companies, Inc. several months ago provides a good example of how BITS and our member companies responded.

- First, we convened information sharing calls among experts in our member companies to discuss the current and potential impact of fraud and identify theft and response strategies of financial institutions that included card re-issuances, increased monitoring of accounts, and customers notification.
- Second, we analyzed the impact of breaches and engaged other organizations to address challenges. While most breaches have involved the compromise of credit and debit card information, the TJX Companies, Inc.'s breach is reported to have compromised check and driver's license information. The theft of this information can be used to access a consumer's checking account and may result in account takeover, counterfeits, new account fraud, and identity theft. We recognized that

there was no known network or industry association that served as the point of contact for the general merchant/retail sector when checking account information has been breached. In light of this gap, we worked with the American Bankers Association (ABA) and Certegy, the check processor for TJX Companies, Inc., to facilitate the distribution of files for Demand Deposit Accounts (DDAs) processed by Certegy from early 2003 to the present. In addition, we reached out to the leadership of the National Retail Federation (NRF) to discuss how the financial services industry and the retail industry can work together more collaboratively prior to and in response to beaches that involve more than credit or debit card information.

- Third, we reminded members of the tools we have developed to help experts in the financial services industry to prevent data breaches and to respond to them more effectively. Examples include the *BITS/ABA Key Considerations for Responding to Unauthorized Access to Sensitive Customer Information, BITS Key Considerations for Securing Data in Storage and Transport,* and *BITS Consumer Confidence Toolkit: Data Security and Financial Services.*
    - BITS and the ABA completed the *BITS/ABA Key Considerations for Responding to Unauthorized Access to Sensitive Customer Information* in 2006 to help financial institutions develop and execute response programs when confidential and sensitive information is accessed or misused by unauthorized individuals. The paper covers the evolving legal and regulatory requirements, potential elements of a response program, and suggestions for managing third party service provider relationships as they relate to data security programs and customer notification.
    - The *BITS Key Considerations for Securing Data in Storage and Transport* paper provides financial institutions with a framework to evaluate the risks associated with the transport and storage of physical media and the destruction or erasure of data on various media. The framework helps risk managers by outlining key questions, identifying risks that can (and cannot) be mitigated, educating key vendors about the needs of financial institutions, implementing appropriately secure storage and transport procedures, and developing effective audit procedures.

- The *BITS Consumer Confidence Toolkit: Data Security and Financial Services* provides an overview of industry efforts to address data security challenges. BITS is currently working on projects to address key management challenges with encryption technologies and the security of wireless technologies.

- Fourth, individual financial institutions communicated with their customers and in many cases issued new cards and/or increased monitoring to detect fraudulent activity.
- Fifth, we maintained contacts with Federal financial regulators and responded to questions about this breach and the impact on related efforts involving information security, outsourcing, business continuity planning, vendor management, payments, and identity theft and fraud reduction.

As another example of promoting secure information technology, we have encouraged government agencies to provide fraud and identity theft prevention tools for use by the industry. For instance, BITS and The Roundtable are encouraging the Social Security Administration (SSA) to provide a robust verification system that will help prevent fraud and identity theft and assist financial institutions in complying with numerous legal requirements. Financial institutions support efforts to establish a consent-based Social Security Number verification program (CBSV) that will allow financial institutions to affirmatively verify a consumer's name, SSN and date of birth against SSA databases. Establishing a real time verification system capable of high volume at low cost would significantly reduce the incidence of identity theft by providing a means of validating key information used at account opening. Consumers would also benefit from industry's ability to verify SSN information by reducing the incidence of fraud and errors.

In July 2006, BITS completed the *BITS Business and Technical Requirements for an Effective and Secure Social Security Number Verification Program to Combat Fraud and Identity Theft.* These requirements provide a framework for cooperation between the SSA and financial institutions to partner on a consent-based verification program that meets the needs of the customers, the industry, and the agency. In July 2006, BITS, The Roundtable, and senior SSA officials met to discuss the business and technical requirements document. Following the meeting, BITS gathered information from member financial institutions regarding their

anticipated participation in a consent-based Social Security Number Verification program. In November 2006 BITS transmitted the results of the survey to members and the SSA. The survey did reveal strong interest from U.S. financial institutions for a CBSV program, but it also indicated several impediments to broader participation in a verification program if changes were not made to the current proposed structure. Financial institutions noted that more would participate in the CBSV program if it:

- is automated;
- does not require paper consent forms;
- has minimum delays in verifications;
- includes a reasonable cost for verification;
- has reasonable record keeping requirements; and
- addresses the need for ID verification processes for non-U.S. citizens.

Participants indicated that the greatest value to the financial institutions via an enhanced CBSV program would be the ability to: verify the identity of an applicant; reduce instances of identity theft; facilitate compliance with the Customer Identification Program (CIP) as required by Section 326 USA PATRIOT Act); reduce losses due to fraud or loan defaults; enhance customer service, as financial institutions would not have to ask customers to go to their local SSA office to validate their SSN; and detect and reduce erroneous tax reporting.

Another important area is government-issued credentials. The DHS recently issued for comment a proposal that outlines the minimum standards for state-issued driver's licenses and identification cards in compliance with the REAL ID Act of 2005. The proposal establishes minimum standards for state-issued driver's licenses and identification cards that Federal agencies could accept for official purposes, such as boarding Federally-regulated aircraft and entering Federal facilities. These standards may also impact financial institutions because financial institutions rely on government-issued credentials to verify identity for everyday functions including opening customer accounts, establishing loans, and hiring employees. Financial institutions also are required by government regulations to identify their clients and gather relevant information before doing business with them. Therefore, it is extremely important that when issuing identification under this proposal, states take all

steps necessary to verify both the identity of the individual and the authenticity of the documents presented to them. Improving credentials, such as state driver's licenses and state-issued identification cards, will provide an important opportunity to improve financial institutions' ability to "know their customer" as mandated by the USA Patriot Act and other laws and regulations.

Responsibility. For many years BITS and our members have urged major software providers to develop more secure software and to accept greater accountability for the software they market and service. This has been part of a larger effort by members of the user community that rely on technology provided by the information technology industry—private-sector companies, universities, and government agencies—to demand greater *accountability* for the security of information technology products and services.

In 2004, BITS hosted a Software Security CEO Summit to bring leaders from the financial services and information technology communities together. We outlined the impact that software vulnerabilities have on the financial services industry, proposed business requirements for software companies, and offered procurement language for financial institutions to use. Following the Summit, we initiated joint work plans with major software providers and developed a best practices guide for patching and testing software.

In 1999, BITS created the BITS Product Certification Program (BPCP) which provides product testing by unbiased and professional facilities against baseline security criteria established by the financial services industry. A product certification, the *BITS Tested Mark*, is awarded to those products that meet the defined criteria. An option is available for technology providers to meet the product certification requirements via the internationally recognized Common Criteria certification schema. BITS has urged DHS to support efforts to enhance product certification programs, including the Common Criteria program run by the National Security Agency (NSA) and National Institutes of Technology and Standards (NIST).

Collectively, these efforts raised the level of awareness of leaders in the technology, financial services and government communities and have resulted in positive change as more technology companies deliver more secure products and services.

Educate: Financial institutions have extensive expertise in educating customers about securing their computers and avoiding the lure of fraudsters. However, financial institutions also know that this is an ongoing challenge. In 2005, The Roundtable's Board of Directors approved the *Voluntary Guidelines for Consumer Confidence in Online Financial Services* and *Critical Success Factors for Security and Awareness Programs of Financial Institution Employee.*[5]

Recently, we have been focusing on making email more secure and reliable. Email is a necessary and important means of communication with customers, business partners, and service providers. We also have learned that without proper protocols, email is insecure and lacks controls that can ensure confidentiality and integrity. In April 2007, we released the *BITS Email Security Toolkit: Protocols and Recommendations for Reducing the Risk.*[6] The toolkit recommends email technology protocols for financial services, Internet Service Providers, and other business partners. We would encourage government agencies to adopt these protocols too and work in partnership with financial institutions, Internet Service Providers and others to increase the security of email as a communication channel.

Procure: In the procurement area, our members are focused on getting the best performance from their investments and ensuring that risks are appropriately managed. An example of this is the Financial Institution Shared Assessments Program (FISAP) which is designed to improve the cumbersome and expensive service provider assessment process. The FISAP is based on two essential documents: The Standardized Information Gathering Questionnaire (SIG), which gives financial institutions a detailed "snapshot" of the security controls at the service provider's location and the Agreed Upon Procedures (AUPs), whose 45 control points can be used by assessment firms or qualified CPAs to create detailed reports regarding the effectiveness of the controls. To date, nearly 50 organizations are involved in the FISAP and there is increasing interest in overseas firms that provide services

[5] See http://www.bitsinfo.org/downloads/Publications%20Page/bitsconscon.pdf and http://www.bitsinfo.org/downloads/Publications%20Page/bitssecaware.pdf.
[6] See http://www.bitsinfo.org/downloads/Publications%20Page/BITSSecureEmailFINALAPRIL1507.pdf.

to financial institutions. The FISAP effort is based on previous work of the BITS IT Service Provider Working group which developed the *BITS Framework for Managing Technology Risk for IT Service Provider Relationships* and the *BITS IT Service Provider Expectations Matrix.*[7] Other major documents produced through the BITS IT Service Provider Working Group include the *BITS Key Considerations for Global Background Screening Practices* and *Key Contractual Considerations for Developing an Exit Strategy.*[8]

Another example is the work BITS did on telecommunications resiliency and diversity. The *BITS Guide to Business-Critical Telecommunications Services* was completed in 2004 based on extensive work by BITS members, participation by all the major telecommunications companies, and involvement by the National Communications System as well as the President's National Security Telecommunications Advisory Council.[9] The guide is a comprehensive tool that is used by our member financial institutions to better understand the risks and strategies for working with telecommunications companies to deliver more diverse and secure telecommunication services.

In recent years, there has been increased focus on authentication which has implications for procurement. In October 2005, the Federal financial regulators issued supervisory guidance requiring financial institutions to improve authentication of electronic banking applications.[10] In response to this guidance and changing threats, financial institutions have implemented stronger authentication technologies and procedures while trying to keep the process simple and convenient for customers.

In late April 2006, BITS participated in the Federal Trade Commission's workshop on authentication. The workshop revealed a number of challenges facing government and the private sector:

---

[7] See http://www.bitsinfo.org/downloads/Publications%20Page/bits2003framework.pdf and http://www.bitsinfo.org/downloads/Publications%20Page/bits2003framework.pdf
[8] See http://www.bitsinfo.org/downloads/Publications%20Page/bitsbcheck.pdf and http://www.bitsinfo.org/downloads/Publications%20Page/bitsexitstrategy.pdf.
[9] See http://www.bitsinfo.org/downloads/Publications%20Page/bitstelecomguide.pdf
[10] See FFIEC "Authentication in an Internet Banking Environment" http://www.ffiec.gov/pdf/authentication_guidance.pdf.

- The complexities of how identity theft is perpetrated and the limitations of authentication technologies currently available to prevent fraud and identity theft.
- Difficulties that governments face in implementing national and state identification programs given the costs and citizen expectations and concerns.
- Promises and perils of biometrics in light of consumer concerns that criminals might access biometric information and perpetrate fraud, in addition to concerns as to how government may use biometric information.
- Greater appreciation for the notion that identity is a relationship and that people adopt identities for different purposes. This creates a dynamic tension for advocates of a national identification system in which there is a unique identifier for each individual.
- Greater understanding of the consumer acceptance challenges and why banks implemented risk-based device authentication technologies to comply with the FFIEC authentication guidance.
- Greater understanding of the importance of interoperability given the many systems used to identify, verify, and authenticate identity.
- Greater use of wireless devices and mobile phones for authentication and for mobile payments.
- Gradual emergence of smart cards for access to government facilities and computer networks.
- Concern over the security of devices given the rise of spyware and botnets and other malware.

Another example with implications for procurement is encryption technology. Encryption is an important and useful tool and a key component of a financial institution's information security programs. However, encryption of data poses a number of significant challenges that financial institutions must consider. First, its application must be measured against the need for interoperability with clients, business partners and regulators, and the ability to access data today as well as to meet recovery and retention requirements in the future. Second, encryption should be used only after identifying the threat before applying a control. For instance, encryption does not protect against abuse of legitimate access to information; whereas better access control requirements, data masking, or other controls could be much

more effective. Third, there are consequences to encrypting data that must be weighed against the benefits. For example, there are potential negative effects on computer networks, the ability to detect intrusions, the reduced speed of computing, and the ability to retrieve data for back-up restoration or business continuity requirements. There also are implications upon mandatory monitoring requirements and the ability to provide regulators records of communications. Fourth, encryption in itself cannot guarantee data security. Given that many of the publicly announced data breaches in recent years were from stolen paper documents or data sold to fraudulent businesses, it is important to recognize that encryption would not have prevented the information from being viewed or compromised. The threshold issue in a compromise is the usability of the compromised data. Encryption is only one class of factors that can affect the usability of data.

Some government agencies do not allow financial institutions to transmit sensitive data in encrypted formats. We encourage government agencies, such at the Internal Revenue Service (IRS), to permit the transmission of encrypted data when our member financial institutions share data with government agencies.

Analyze and Research: In the analysis and research areas, financial institutions have encouraged the government and academic community to collect and analyze information on the costs and impact of information security risks, vulnerabilities and threats. In 2006, the Departments of Justice and Homeland Security initiated a National Cyber Security Survey (via The RAND Corporation). BITS supported this effort and encouraged our members to participate in this survey. Our hope was for more accurate data on the cybersecurity challenge and its impact on society. Since initiating the study last year, our members have not received feedback or results of the study.

In 2005, BITS urged the FSSCC to establish a committee to outline research and development priorities based on recommendations in the Administration's National Strategy to Secure Cyberspace and National Strategy for Physical Protection of Critical Infrastructures and Key Assets. The FSSCC's R&D Committee, working in partnership with the Treasury Department, issued a list of research challenges designed to further strengthen the security and resilience across the sector and then published a research agenda.

The FSSCC research agenda identifies the most promising opportunities for research and development initiatives in the following areas:[11]

- Secure Financial Transaction Protocol
- Resilient Financial Transaction System
- Enrollment and Identity Credential Management
- Suggested Practices and Standards
- Understanding and Avoiding the Insider Threat
- Financial Information Tracing and Policy Enforcement
- Testing
- Standards for measuring ROI of CIP and Security Technology

The FSSCC is working in partnership with the Treasury Department and Federal financial regulators involved in the Financial and Banking Infrastructure Information Committee (FBIIC) to develop the Sector Specific Plan (SSP) for the Banking and Finance Sector and research and development priorities. The Banking and Finance Sector Specific Plan SSP was completed earlier this year and joined with 16 other sector specific plans as part of the National Infrastructure Protection Plan (NIPP). The Banking and Finance SSP outlines a strategy for working collaboratively with public and private sector partners to identify, prioritize and coordinate the protection of critical infrastructure, including information security. It describes how this public-private partnership has become part of the fabric of our sector over the past four years and identifies areas where work remains to be done.

Enforce. Under the category of encouraging law enforcement to enforce, investigate and prosecute cyber crimes here and abroad, the financial services industry is playing a leadership role. Financial institutions have an obligation under existing laws and regulations to file Suspicious Activity Reports on computer crimes, identity theft and others. This information is a major source for regulator and law enforcement agencies to investigate crimes. Another example that is purely a private sector driven effort is the work of the ITAC in partnering

[11] For more information, please see the current FSSCC Research Agenda at: www.fsscc.org/reports/2006/Research_Agenda_Booklet_061108.pdf

with law enforcement to catch and convict criminals while assisting victims of identity theft. With the consumers' consent, ITAC shares information about these crimes with the United States Postal Inspection Service (USPIS) and hundreds of other law enforcement agencies through the FTC Consumer Sentinel database. Data supplied by ITAC is helping law enforcement catch the individuals who commit these crimes. The USPIS reports that for the fourth quarter of 2006, data from ITAC helped produce eighteen arrests and the execution of three search warrants. The success of law enforcement efforts is heavily dependent on front-line law enforcement officers having the knowledge and forensic skills essential to the investigation of computer-based crime. For that reason, ITAC is working closely with the United States Secret Service and the Alabama District Attorneys Association on the National Forensic Computer Institute which will train hundreds of law enforcement personnel each year in computer forensic techniques.

Conclusion

I would like to close by stating that securing information is no easy task and there are no simple solutions. Securing information and protecting privacy is an ongoing process. It requires constant vigilance, constant enhancement to address new and emerging threats, and collaboration with partners. Members of BITS are sharing information, analyzing threats, creating best practices, urging the software and technology industries to do more to provide more secure products and services, and combating fraud and identity theft. These efforts are helping the financial services industry mitigate some of the risks facing the financial services industry and can be applied by government agencies in complying with the goals of FISMA. Our members also want to encourage the Congress to improve information security by urging government agencies to develop more secure credentials that can be used to identify individuals, by implementing a Social Security verification program to reduce fraud and identity theft, and by encouraging government agencies to permit financial institutions to transmit sensitive information in encrypted formats.

Thank you for the opportunity to testify before you today.

APPENDIX: PREPARE: RECOMMENDATIONS FOR GOVERNMENT

Promote. Government can play an important role in promoting the importance of secure information technology. Also, government should do more to facilitate collaboration among critical infrastructure sectors and government. Some sectors, such as financial services, are heavily regulated and supervised to ensure that customer information is protected and that financial institutions operate in a safe and sound manner. Examples of actions the government can take include:

- Government should lead by example by ensuring that the issue of cyber security receives adequate attention in the Department of Homeland Security.
- Strengthen information sharing coordination mechanisms, such as the Information Sharing and Analysis Centers (ISACs), by ensuring adequate funding is made available to Federal agencies sponsoring such organizations. Information sharing and trend analysis within a sector is essential to protecting information security and responding to events. Information sharing among sectors is equally important as cyber threats sometimes reach some sectors before others.
- Create an emergency communication and reconstitution system in the event of a major cyber attack or disruption of information networks. Such an attack or disruption could potentially cripple many of the primary communication channels. To allow maximum efficiency of information dissemination to key individuals in such an event, a thorough and systematic plan should be in place. The financial services industry employs a system for industry-specific events through the BITS/FSR Crisis Communicator. Other organizations have developed similar communication mechanisms. These emergency communications programs should be examined as potential models for a national cyber security emergency communication system.
- Reform of the Common Criteria/National Information Assurance Partnership (NIAP). The current software certification process is costly, inefficient, used on a limited basis by the Federal government, and virtually unknown to the private sector. NIAP should be reformed so that it is more cost effective for vendors to seek certification while ensuring consistent Federal procurement practices and expanded commercial adoption of NIAP-certified products. The BITS Product Certification Program may well be able to serve as a model.

Responsibility. Government should promote shared responsibility between suppliers and end users for developing, deploying, and maintaining secure information networks. Government can play an important role in establishing incentives and making producers of software and hardware accountable for the quality of their products. Examples of actions the government can take include:

- Provide tax or other incentives for achieving higher levels of Common Criteria certification. Incremented incentives would help to compensate companies for the time and cost of certification. This should encourage certification and increase the overall security of hardware and software.
- Provide tax or other incentives for certification of revised or updated versions of previously certified software. Under Common Criteria, certification of updated versions is costly and time consuming. Incentives are necessary to ensure that all software is tested for security
- Require software providers to immediately notify ISACs of newly discovered cyber threats and to provide updated information on such threats until an effective patch is

provided. It is vital that critical infrastructure companies receive immediate notice of serious vulnerabilities.
- Establish requirements that improve the patch-management process to make it more secure and efficient and less costly to organizations.

Educate. Communicate to all users of information technology the importance of safe practices. Public confidence in e-commerce and e-government is threatened by malicious code vulnerabilities, online fraud, phishing, spam, spyware, etc. Ensuring that users (home users, businesses of all sizes, and government) are aware of the risks and take appropriate precautions is an important role for government and the private sector.

Procure. Using its purchasing power and leveraging security requirements and best practices developed by the public and private sectors, government can play an important role in encouraging the IT industry to deliver and implement more secure systems. Examples of actions the government can take include:
- Require high levels of cyber security in software purchased by the government through procurement procedures. Extend such requirements to software used by government contractors, subcontractors, and suppliers.
- Provide NIST with adequate resources to develop minimum cyber security requirements for government procurement. NIST should include software developers and other stakeholders in the standard-creation process.

Analyze. Government should collect information and analyze the costs and impact of information security risks, vulnerabilities and threats and provide this analysis to policy makers. Examples of actions the government can take include:
- Assign to the Commerce Department or another appropriate agency the responsibility of tracking and reporting such costs and their impact on the economy. Measuring and making these costs transparent will aid law makers and regulators as they assign resources to cyber security programs.

Research. Government can play an important role in funding R&D in the development of more secure software development practices, testing and certification programs. In addition, training future generations of programmers, technicians and business leaders that understand and manage information security can be accomplished by establishing university and educational/certification programs. Government can help by facilitating collaboration with the users and suppliers of IT to develop standards for safe practices. Examples of actions the government can take include:
- Enhance DHS, NSF, and DARPA cyber security R&D funding.
- Carefully manage long- and short-term R&D to avoid duplication.
- Establish a mechanism to share educational training and curricula.

Enforce. Law enforcement must do more to enforce, investigate and prosecute cyber crimes here and abroad. Examples of actions the government can take include:
- Enhance criminal penalties for cyber crimes.
- Make cyber crimes and identity theft enforcement a higher priority among law enforcement agencies.

Mr. CLAY. Thank you so much, Mr. Carlson.

Mr. Lewis, please proceed.

STATEMENT OF JAMES ANDREW LEWIS

Mr. LEWIS. Thank you, Mr. Chairman. Thank you for this opportunity to testify.

The committee is aware of the damage done to U.S. interests in national security by the successful penetrations of Federal networks we have seen in the last year or so. Much valuable information has been lost. We don't want to overstate the risks, but at the same time we don't want to ignore the damage.

We should note that an agency's FISMA score is largely irrelevant to telling how well it is able to withstand these attacks.

The growing sophistication of software tools available for cyber crime and espionage increases the risk to Federal systems. Recent events in Estonia, which is a small country attacked by unknown hackers, shows how we face probably a greater threat than we did when FISMA was enacted.

We can draw some lessons from the Estonian experience. They responded calmly and rapidly to the attacks, but they are a small nation. The United States is larger and operates many more networks. That means in some ways we are a more difficult target, but at the same time we may not be as efficient in our response.

The question of efficiency goes to the heart of FISMA. The U.S. Government operates hundreds of thousands of computers. We talk about an enterprise architecture, which means a corporation under a powerful CEO where all the business units are unified in their efforts, but I don't think this is possible for the Government. No single agency has control of the Federal networks.

Congress passed FISMA to bolster network security within the Federal Government. FISMA provides a framework for security and mandates yearly audits. The intent behind FISMA was good, but an agency can get good marks in FISMA and still be vulnerable. This is despite much good work in recent years to improve security.

We need to ask whether FISMA is still relevant. One way to answer this question is to look at the process. FISMA involves the production of reports. The reports certify whether certain standards are being met. These standards, if followed, may improve security or they may not. FISMA is a direct measurement of compliance with processes and an indirect measurement of security. If we asked agencies whether or not their networks were secure, as measured by penetrations or data loss rather than by whether they follow certain standards, their answers would produce more accurate results.

Another way to look at FISMA is to ask how the technology has changed. The most important change, as you heard from Mr. Kurtz, lies in how the Internet is used. There are new Web applications. Federal agencies use some of these, such as wikis. Other applications, such as Web-based services, are not yet widely used, but because of their cost advantages they will be. Any re-examination of FISMA should update the act to allow for the evolution of technology.

In my view, FISMA needs an overhaul. One way to do this would be to replace FISMA's emphasis on certification, with performance-based measures that focus on vulnerability to attack. Revising FISMA to focus on performance and to ask how many times a system was probed or penetrated, what the vulnerabilities were that allowed for a successful attack, and what steps were taken to rectify these vulnerabilities might be the single most important change that Congress could make.

Another way to improve FISMA would be to link it to mandatory consequences. A successful attack or a low score should trigger a requirement for agencies to reprioritize and reallocate funding for information security.

By itself, even a FISMA that worked perfectly would be insufficient to secure Federal systems. A revised FISMA has to be part of a larger strategy. The elements of this strategy should include: increased accountability and responsiveness by agency leadership; adequate funding; use of the acquisitions process; and increased emphasis on protecting information rather than networks.

Using the Federal acquisitions process to encourage suppliers to make IT products more secure could be very beneficial. For example, the Government could give preference to commercial software made with industry best practices for security.

I want to conclude by saying although there has been progress in recent years, better Federal organization would also help improve information security. We are better off than we were 10 years ago, but not all agencies have seen equal improvement. Despite FISMA, cyber security remains a low priority for many agencies. Much remains to be done.

Let me tell you an encouraging story, though, to finish up, Mr. Chairman. We faced a similar challenge in the 1980's when the United States discovered that its communications over telephone networks were not secure. The United States began a program then to secure sensitive voice communications. Within a few years this program, which was implemented by the National Security Agency, had succeeded in securing communications. There are major differences, of course, between telephone networks and the Internet, but the lesson of identifying a problem, assigning its resolution to a competent agency, and moving aggressively with adequate funding to fix it offers a model for how to improve information security.

My view is that, with better organization and strategies, we can make Federal information systems more secure, and an improved FISMA can play an important part of this effort.

Thank you.

[The prepared statement of Mr. Lewis follows:]

Testimony
House Committee on Oversight and Government Reform
Subcommittee on Government Management, Organization and Procurement
And the
Subcomittee on Information Policy, Census and National Archives
"Federal IT Security: The Future for FISMA"
James A. Lewis
Center for Strategic and International Studies
June 7, 2007

Thank you for this opportunity to testify on this important subject. Improving information security in the Federal Government is a crucial task for the United States. Recent events in Washington and in Estonia highlight the importance of this task. In my testimony, I will briefly discuss the threats we face; the status of federal information security; ideas about FISMA and additional ideas for improvement.

I am sure that the Committee members are well aware of the damage done to national security by successful penetrations of Federal networks. Much valuable information has been lost to our opponents. This damage is different from the sort of risks one often hears from the IT community – the risk that a cyber attack will produce physical damage in the US – the electronic Pearl Harbor scenarios of the 1990s are entertaining, but not a useful guide for policy or legislation. That kind of risk is small. Our concerns should be with the loss of sensitive information and in the disruption of key services and data as a result of hostile intrusions into our information systems.

Our adversaries have exploited vulnerabilities in Federal networks to obtain information of military and economic value. This has been going on since at least the late 1980s. The most recent episode involved penetration of networks at various agencies, including Commerce and State, and the downloading of masses of information. We should note that an agency's FISMA score was largely irrelevant to how well it was able to withstand these penetrations.

We do not want to overstate the risks. At the same time, we do not want to ignore the damage to national security from intelligence gathering, economic espionage and the theft of technological or military information. In addition to the theft of government information damages U.S. security and economic leadership, there is also a real risk that opponents will seek to disrupt government activities by scrambling data and by creating confusion and uncertainty. It is these kinds of informational attacks that pose the risk of even greater harm to the U.S. in the future.

The rapid increase in the sophistication of software tools available for cyber crime and espionage increases the risk of these attacks. A flourishing network of professional criminal has assembled an arsenal of tools. Criminals create and use 'bot' networks, where programs automatically search the internet for vulnerable computers and then implant program that make the infected computer a 'robot" available for attacks or spamming. Their ranks now include skilled programmers, and cryptographers who carefully monitor and test their own weapons. They also constantly probe networks and software products for new vulnerabilities to exploit. Intelligence agencies, of course, can draw upon their skills and tools offered by cyber criminals (botnets, for example, can be rented by the hour), recruit hackers to carry out missions, and supplement criminal talents and tools with their own specialized skills.

The events in Estonia show how foreign governments, criminal organizations or cyber protestors can use the tools of cybercrime to disrupt key services. Hackers, probably Russian, and probably encourage by the Russian government, used "botnets" to flood Estonian government and business networks. Botnets are a collection of computers on which a cybercriminal has been able to illicitly load software that makes the computer a 'zombie,' carrying out the criminal's instructions without the computer's owner even being aware that his or her machine is being used. Millions of computers are around the world are infected. The effect of these botnet attacks, which peaked perhaps a thousand a second, meant that the targeted Estonian networks were unable to respond to legitimate queries from employees, citizens and customers and in some cases had to shut down.

There are several lessons we should draw from the Estonian experience. The first is that while the attack was disruptive, it did not turn Estonia into a quivering mass of jelly. There was neither terror nor destruction. The Estonians responded calmly and rapidly to the attacks. Many sites had restored service, at least to minimal levels within a day or two of the attacks. In part, this was because the kind of attack used against Estonia – called 'denial of service" is not the most damaging form of attack. A more determined attacker would have penetrated Estonian computers and scrambled the information located on them. This is a much more damaging tactic for information warfare and it is the kind of attack about which we should worry.

Estonia is a small nation that has paid much attention to e-government. The U.S. is much larger, and operates many more networks. This makes it a more difficult target, but at the same time, I am not sure that we would be as efficient in our response as the Estonians. In the last few years, the Department of Homeland Security has undertaken several exercises to test private sector and Federal responses to cyber attack. These exercises point to improvement in our defenses, but are not conclusive.

The question of efficiency goes to the heart of the FISMA problem. The U.S. government operates thousands of computer networks to which hundreds of thousands of computers and other devices are attached. We talk about an "Enterprise architecture,' a term from business that entails restructuring a corporation under a powerful CEO to unify the efforts of its business units, but this sort of restructuring and control is not possible for the federal enterprise. No single agency the ability to control this multifaceted complex of networks.

The tools for managing this complex federal information system are limited. The Office of Management and Budget (OMB), the Defense Department and the Director of National intelligence each have primary responsibilities for cyber security. Of these lead agencies, OMB faces the most difficult task. Unlike DOD or the DNI, where the component agencies have relatively similar missions and are innately concerned with security, OMB faces agencies with disparate tasks and structures. It is to these "civilian" agencies that FISMA is most useful as a guide, because in the absence of FISMA, cybersecurity would likely receive even less attention that it receives now.

Congress passed the Federal Information Security Management Act of 2002, FISMA, to bolster computer and network security within the Federal Government. FISMA provides a framework for security and mandates yearly audits, where Agencies report to OMB on their efforts at information security and their compliance with a collection of standards, laws, rules and processes produced over the years by Congress, the Executive Branch, and the National Institute for Standards and Technology – NIST. The reports include an independent

evaluation, either by an Agency's Inspector General or by an outside auditor hired to write the various required reports.

The intent of FISMA was good. There are benefits from FISMA. Unfortunately, an agency can get good marks in FISMA and still be vulnerable. This is despite much good work in the Federal government in recent years to improve the security environment. In assessing why this is so, we need to ask whether FISMA has become irrelevant.

One approach to answering this question is to look at the FISMA process. FISMA involves the production of reports and other documentation. The report certifies whether certain standards are being met. These standards, if followed, may produce security, or they may not. FISMA is a direct measurement of compliance with processes and an indirect measure of performance. In effect, FISMA does not directly measure security, and if we asked agencies whether or not their networks were secure, as measured by penetrations and data loss, rather than if they were following certain processes or standards, their answers would produce different and better results than FISMA. As many have said, focusing FISMA on performance and outcomes would be an improvement over the current process.

Another way to answer the question of whether FISMA is still relevant or useful is to consider how technology has changed in the last five years. The most important lies in how the internet is used. FISMA came at a time when the Government was moving from a mainframe environment to what are called client- server networks. This focus on agency networks was appropriate at the time FISMA was written, but it is increasingly less valuable for security as more of the activity happens outside of the agency's network. Some of this change in focus involves what some people call "Web 2.0." Web 2.0 sounds like a marketing term, and to some extent, it is, but it also describes new web applications that are seeing growing use. Federal agencies use some of these applications, such as wikis, blogs, and podcasts. Other applications, such as a reliance on web-based services (those accessible over the Internet) rather than on services hosted at an agency's own computer networks, are not yet widely used in government.

This is the direction technology is taking. In the future, when Federal employees do their work, they will need to access many different networks outside of their own agency. Agency networks will need to be more open to enable information sharing. FISMA is not well suited to this emerging Internet environment. While are many impediments to getting the Federal government to adopt the most productive and efficient processes found in the private sector, including workforce rules, the budget and acquisitions process, and a preference for low risk solutions, FISMA is probably an impediment as well. Any re-examination of FISMA should update the Act to allow for the evolution of technology and to move away from a focus on securing the agency network as the way to produce information security to a focus on securing the information itself.

FISMA is the tool we have now for encouraging agency action and until it is replaced, it is the tool we must use. Since FISMA measures the wrong things and does not accurately reflect the real state of information security at an agency, the answer to the question as to whether it is still useful is: FISMA needs a thorough overhaul.

One way to do carry out this overhaul would be to replace FISMA's emphasis on certification that an agency had complied with various standards with performance-based measures that focused on vulnerability to attack. These methods could include looked to , such as creating a Federal "Red Team" that periodically tested each agency's defenses to find vulnerabilities.

The result of a Red team exercise might do better at identifying vulnerabilities that could be fixed than a process that assumes that compliance with a standard produces security. Revising FISMA to focus on actual performance measures, such as how many times a Federal information system was probed or penetrated, what vulnerabilities allowed for a successful attack, and what steps the agency had taken to rectify these vulnerabilities, might be the single most important change that the Congress could make.

One way to make improve FISMA or any successor act would be to link it to mandatory consequences. FISMA is not action forcing. A low FISMA score is painful now for Chief Information Officers, but this is not enough. If gangs of hostile foreigners broke into Federal buildings, trashed offices and carted off dozens of file cabinets, it would be a scandal. When the same thing happens in cyberspace, we tend to either downplay it or simply throw up our hands. Responsibility for a low score or a successful attack should lie with the head of an Agency, not just the Chief Information Officer. A successful attack or, if we continue to use FISMA, a low score, should trigger a requirement for agencies to reprioritize and reallocate funding to counter information security risks, consistent with appropriations laws.

By itself, FISMA will be insufficient to secure Federal information systems even if it is revised. A revised FISMA should be part of a larger strategy for Federal information security. The elements of this strategy should include increased accountability and responsiveness by agency leadership, adequate funding for security, use of the federal IT acquisitions process, and increased emphasis on protecting information rather than networks.

Using the Federal Acquisitions process to encourage suppliers to produce more secure IT products should also be part of a Federal information security strategy. In this regard, FISMA is just one of several standards and processes already used to evaluate products or processes for security. Other leading standards include the Common Criteria, the Carnegie Mellon Software Institute's Capability Maturity Model (CMM), the ISO 9000 series, ISO 19779, SAS 70, and NSTISSP 11. In addition, the Department of Homeland Security is developing a new evaluation process for software products. All of these standards have their strengths, but the common industry view is that they are inadequate for increasing security. As with FISMA, a Federal information system can use products or networks that have passed these various standards and yet still be vulnerable.

The Common Criteria process is the most important of the existing processes for certifying software for sensitive Federal applications. Like FISMA, it is expensive, cumbersome, requires large amounts of documentation, and focused on certifying processes rather than results. A more flexible approach that made the use of existing industry best practices for coding secure software one factor for consideration in acquisitions of commercial software could help to improve security. Part of any larger strategy for security Federal Information systems should be to develop and implement new ways to use acquisitions to incentivize the IT industry to supply more secure products.

For example, commercial software that was produced using industry best practices for security could be given preference in acquisitions. These practices include security training for programmers; strong management procedures that provide oversight and; an independent review of code for security issues (including the use of software assurance tools); and testing of products by red teams or penetration efforts. Many companies have adopted these practices, but acquisitions rules do not take this fully into account. The Federal IT acquisitions can be a powerful source for change in creating secure commercial products.

Identifying the best practices for federal network security, turning those into common performance standards, and finding a better way to communicate and enforce those performance guidelines across agencies would improve security.

Although there has been progress in recent years, better Federal organization would improve information security. The Departments of Homeland Security and Defense, the Office of the Director for National Intelligence, the Federal CIO Council, the Homeland Security Council, the National Security Council, and the Office of Management and Budget all play a role in developing and overseeing policy for securing federal networks. Rationalizing and streamlining the governmental processes for cyber security is essential. The National Security Council has created a new Policy Coordinating Committee for Cybersecurity and making this becomes a focal point for driving strategy and implementation to improve security.

Let me conclude by noting that in looking at the security of Federal networks, it is fair to say that while the U.S. is better off than it was five years ago or ten years ago, not all agencies have seen equal improvement. Despite FISMA, remains too low a priority and an afterthought for many domestic agencies. Much remains to be done.

We can draw some encouragement, however, from a similar challenge the U.S. faced in the 1980s. At that time, Federal government voice communications over telephone networks were not secure and that our opponents were exploiting them to obtain sensitive information. In the mid-1980s, the federal government began a program to secure its sensitive and classified voice communications. Within five or six years, this program, which was implemented by the National Security Agency, had considerable success in securing the most sensitive Federal communications.

There are major differences, of course, between securing the telephone network of twenty years ago and what is needed to secure information today. There are many more networks and participants, much more data, and the technology is more complex and diffuse. That said, the lesson of identifying a problem, assigning its resolution to a competent agency, and moving aggressively with adequate funding and White House attention to fix, it, offers a model on how to address information security.

The Federal government may be the most challenging environment in the world for cybersecurity due to its diversity and size. The U.S. will need to undertake a number of complementary measures to reduce its vulnerabilities, but with better organization and strategies, we can make federal information systems more secure. An improved FISMA could be an useful part of this effort. I thank the Committee for this opportunity to testify and will be happy to answer any questions.

Mr. CLAY. Thank you, Mr. Lewis, for your testimony.

Chairman Towns has rejoined us, and I will go to Chairman Towns and recognize him for questions.

Mr. Towns.

Mr. TOWNS. Thank you very much. I really appreciate this hearing.

One of the biggest weaknesses in security for the Federal Government has been the use of portable devices—laptops, computers, disks, USB drives, etc.—where the data goes out the door with the user, and the only protection is hoping that the user doesn't lose the device or have it stolen. In other words, basically it has been a human problem more than a technical problem.

How does industry deal with that, Mr. Bond?

Mr. BOND. I will take a first shot, and I am sure the financial services industry would have some, as well, Mr. Chairman. Thank you for the question.

I think that one difference between the private sector and public sector in this regard is there is a deeper level of continuous assessment of where the network is extending, to which devices, a greater level of authentication within the leading companies and best practices to know which devices are connecting to their network, whom they belong to, are they authenticated.

The Federal Government is beginning to move down that path with a number of efforts like HSPD–12 and others to be able to authenticate who is entering a building, much less who is using a PC, a thumb drive, or whatever. So it is a long road. I think there is much to learn from the private sector in this regard, and probably much to learn from the financial services industry to get to the level of continuous assessment and confidence that you need in such a large enterprise and such a large network.

Mr. CARLSON. I would also add to that. The nomenclature of information security, you always talk about it in terms of people, process, and technology, so all three of them are equally important in terms of how you secure information.

Certainly in the financial services industry we have been a target of fraudsters to go after information, to hack into systems for financial gain. Our industry has really responded very aggressively over the past 10 years to tighten systems, to improve authentication, to encrypt more information, to mask data, to restrict the use of Social Security numbers in the verification process. So collectively those efforts are making good progress in terms of making it more difficult to access the information.

There is also the human component of it, and that requires a lot of education on the part of employees, contractors, and consumers that are using the devices to access, say, their bank, or users that are accessing Government facilities, to make sure that they are doing the right thing in securing their portion of the chain.

Mr. LEWIS. If I could just add, Mr. Chairman, I do think this is, in some ways, a problem that our technological fixes for, this should not be a big deal. If you have better authentication, if you have better encryption, losing a laptop should not mean the loss of valuable information. That is sort of the normal practice in the high-tech industry, and we need to see the Government move more rapidly to adopt those practices.

Mr. KURTZ. If I may add to what everybody has offered, I think, first and foremost, we do not want to have Federal employees and contractors tethered to their desks and not be able to be mobile with their devices, so laptops, the ability of Federal employees to be mobile and do work from all places is really important. And to the technical solutions, finally we have guidance from OMB as of last summer to encrypt it. We need to encrypt it at rest and in transit, and we should move down that road far more quickly than we have in the past. We also must increase authentication.

As Mr. Bond said, we have HSPD–12, a directive to use greater authentication across Federal agencies and with contractors. Both of those areas should receive great priority.

And, finally, unlike the private sector, there are not necessarily consequences for using a laptop. In the case of VA, the individual was ultimately dismissed, but a lot of laptops are lost and there really are no consequences for those who actually use them. In the private sector, obviously there could be consequences.

Mr. TOWNS. Thank you very much.

Let me ask, if we were to change FISMA, if we were to strengthen, what is the one thing that we need to do? I would like to go down the line on it. There are two things that you must say, feel free to do so, but how we might be able to strengthen it.

Mr. BOND. I offered six when you weren't here, so I will pick my favorite.

Mr. TOWNS. I am sorry.

Mr. BOND. No, I appreciate your leadership on this, Chairman Towns, and appreciate your having the hearing.

I guess if I had to pick one of those, though, I think I would say an annual risk assessment by the agencies that included classified information and input from the latest and greatest in the private sector. We know there are some agencies who either don't have the personnel, the communication facilities, or whatever, to receive even classified briefings to go into the risk assessment, and so we must be missing it. That is what I would say, No. 1.

Mr. TOWNS. OK. Thank you.

Mr. KURTZ. Most likely, close to what Mr. Lewis talked about, and that would be a requirement for annual vulnerability assessment, a real red team, against each Federal agency, where we are also getting reported on the number of attempted attacks and penetrations against an agency, as well as what they are doing to mitigate those problems. It really isn't a strong requirement to do that today.

Mr. TOWNS. Yes.

Mr. Carlson.

Mr. CARLSON. Yes. I would add I think it is important to make sure that the program the Government puts in place, whether it is at the agency level or across the board, has at its heart collaboration, that it supports it, that it encourages it within the organization, but also across the Government and with the private sector.

I think there also needs to be a program that is very much risk-based and forward-focused. We can't be focused on solving yesterday's problems at the expense of not focusing on tomorrow's problems. And this space is moving so rapidly. Technology moves forward quickly. There is a tremendous amount of competition, and

I think the best thing the Government can do can also be a driver for responsible practices by using its vast procurement power to purchase products that have high security standards, that are tested, that are going to meet the needs of the Government and the people that the Government is entrusted to protect. So using that procurement power could be very, very forceful in terms of driving the industry forward.

Mr. LEWIS. Good question. Thank you. I would say, following on Mr. Kurtz, performance base scores tied to mandatory action. Test the system. Don't tell me you complied with some standard. Test the system, and if you fail you are required to do something to fix that. That is what we need to do.

Mr. TOWNS. Thank you very much. I yield back, Mr. Chairman.

Mr. CLAY. Thank you, Mr. Chairman.

Mr. Bond, a critical element of FISMA is for agencies to develop a risk assessment of their systems in order to develop or integrate effective security policies and applications for them. With this in mind, please characterize the vendors' roles and responsibilities in developing and implementing secure networks and applications throughout an agency. And isn't the mitigation of risk a shared duty or responsibility between both agency personnel and the vendor community?

That is two questions.

Mr. BOND. Yes. Thank you, and let me try to get there on both of them.

I think absolutely that the leading contracting companies in this space feel that they share the mission, that this is a critical mission for the country, of which they are a part, and that they want to make sure the Federal Government succeeds as much as humanly possible. So I think it is very much a partnership.

It is also a partnership because so much of the network—and we heard testimony about you are only as good as your weakest link—so much of the network is in private sector hands, so this is de facto a private/public partnership.

I think, in terms of the responsibilities, there is some work that needs to be done there to clarify that, even under FISMA, which assigned some responsibility to the head of the agency. How that plays out then at the contractor level, who has which responsibilities, is sometimes not as clear as it should be in the contracted relationships, so I think there is some work to be done there.

Mr. CLAY. Thank you for that.

Mr. Kurtz, what remedies would you offer to NIST and OMB for providing stronger or more timely guidance? How can new guidance or security controls be added in a real time environment?

Mr. KURTZ. Well, first of all I would, in large part, commend the work of OMB and NIST. I think NIST is internationally recognized for the work that it does, but at the same time the standards process is slow and methodical. So in that case I think OMB has a special responsibility to be, if you will, more agile and more responsive.

I think Karen Evans has done an excellent job, but I also think we kind of learn the hard way. If we look at the directive to encrypt, the directive to authenticate, it was only after we had real problems.

So I think annual guidance update that OMB carries out that Karen talked about earlier today is incredibly important, and that we ought to be used to continue to make sure the implementation of FISMA, the execution of FISMA is strong and to the point.

The classic example I would give right now is the migration to Web-based applications, software as a service. Right now the Government is not in the right place on that. They are way behind the private sector. There is a huge migration underway, and FISMA and implementation of FISMA is not prepared for this migration. There are huge losses in efficiency and value to the Federal Government that are going on right now because we are not agile enough in updating that guidance so agencies can take advantage of it.

Mr. CARLSON. Pardon my lack of knowledge on that, but you and other witnesses have mentioned software as a——

Mr. KURTZ. Software as a service.

Mr. CLAY. As a service. Explain what that is.

Mr. KURTZ. I will take a shot, and then I will turn to others on the panel.

Essentially, we lived in a world where you had software on your computers, applications that sat on your computers that you would pull up in order to create a Word document, Excel spreadsheet, or whatever it would be. Now we have software applications and data that is being stored offsite. So, just like you do online banking, it is much the same, where you are tapping in to software and data that is held elsewhere.

The real value of, if you will, service on demand via subscription is that the Federal Government is no longer assuming those enormous costs of maintenance and upgrade. It is, if you will, the provider's job to take care of that. It is the provider's job to maintain the software, to upgrade it, and it is a fairly seamless process. Great efficiencies could be made available to the Federal Government if they were to pursue that.

Phil, you may have a much better description than I.

Mr. CLAY. Mr. Bond, do you have anything to add? Did he pretty much describe it?

Mr. BOND. Yes. I think you have probably pretty well got that. I think we, on this side, are sometimes guilty of geek speak, but it looks like you got it.

Mr. CLAY. I think I got it. Thank you for that.

Mr. LEWIS. Can I just add one thing on that, Mr. Chairman?

Mr. CLAY. Mr. Lewis, please, if you have something to add.

Mr. LEWIS. We actually use it at my work. We do our time and attendance and our payroll on it. We shifted. People were worried about security at first, and we have been doing it now for 4 or 5 years without a problem, so think about that. Instead of doing a time card and filling it in here we do it on the Internet. It goes to some company. I don't remember their name. They do it all for us.

What we see in the press like the Wall Street Journal is this can bring savings of 20, 25, 30 percent, so it is significant.

Mr. CLAY. And Mr. Lewis, the company secures that data, that information for you?

Mr. LEWIS. Very much so, sir. We looked into it.

Mr. CLAY. Mr. Bond, do you have something to add?

Mr. BOND. Yes. I would just add very quickly they secure the data as well as the transmission of it to make sure that it comes to you safely. While I agree with Mr. Kurtz that the Federal Government is behind on this and certainly NIST is well positioned to be between the private sector and Government to help understand how to process information in the future, I do want to note for the record the Department of State, Treasury, a number of State governments, county governments have deployed software as a service model, so it is being done, but I can't even say we have scratched the surface yet.

Mr. CLAY. But we ought to urge our Government to take a look at that. Thank you.

Mr. Carlson, while FISMA offers us a good baseline of information to work with, there are significant concerns that we are not gathering better performance data from our networks in a real time environment. Has BITS or other industry efforts sought to develop better metrics or data gathering methods for its systems?

Mr. KURTZ. We have a lot of discussion among experts within our member companies about how to manage information security related risks, so through those discussions we kind of coalesce around a number of different approaches that the industry finds useful and effective. Many of those have been published in some of the guides that we have put out, either as metrics tools or efforts to identify where there may be gaps in the program that an individual institution has in place.

I would also add that our environment is a little bit different in that we also have regulators that constantly come in and do audits of financial institutions and determine whether or not those controls are adequate to meet the information security needs that the institution is dealing with. So there is almost like a double layer approach. Institutions do the risk analysis, develop the metrics, come up with the solutions that meet their risk-based environment, and then regulators come in and do an evaluation to see whether or not they are adequate.

Mr. CLAY. Thank you for that response.

Mr. Lewis, we have all been reading about the recent cyber attacks in Estonia, which are primarily distributed denial of service attacks. There remains some uncertainty regarding the ultimate source of the attacks, which were delivered using botnets. Could you offer us some comment on, one, the ability of our agency systems to handle such an attack, and, two, the effectiveness of FISMA compliance as a means to develop some level of assurance that such attacks could be withstood?

Mr. LEWIS. Certainly, Mr. Chairman.

Unfortunately, I think if you were to look at the Federal Government you would probably find that the ability of agencies to respond to this kind of attack would be very uneven. Some could do quite well. Others, as we known from recent events, would probably have real problems.

Now, let me note that in Estonia, there were these attacks. They were massive. But the government IT people there were able to bring most services back online within a few days. So it was disruptive, but it didn't destroy Estonia or lead it to collapse.

We would also not face collapse or some terrible outcome, but there would be disruption. We have seen that now. There are some agencies that were attacked a few months ago and are still having difficulty accessing the Internet, such as, I believe, the Department of Commerce.

Where does FISMA fit into this? Right now it may not be as useful as we might like. FISMA measures how well people conduct certain certifications, how well they construct their systems, how well they document what they have done. But I am not sure how useful it is in measuring their ability to actually deal with an attack, so this would be an area where FISMA, although it is very beneficial, it focuses attention, it is an area where we could improve it.

Mr. CLAY. Thank you for that response.

Mr. Carlson, one of the programs BITS has established is the BITS product certification program to test IT products against security criteria developed by the financial services sector. Please outline for us how this program works and whether there are components that could be adopted or recognized by the Federal Government for its systems.

Mr. CARLSON. Yes. The program was established about 8 years ago as an effort to try to provide a forum to signal to the software industry what are baseline security needs for the financial services industry. It evolved over time into a program in which the industry would lay out these baseline security requirements in a number of different areas and then provide a means in which a software company could come in and test, pass or fail, whether or not it met these baseline security requirements.

We then made some modifications to it to be compatible with a common criteria program, which is a program that the NSA and NIST run, so that a company could go through both the common criteria program, the BITS product certification program.

So there are many elements of it, and we have shared our work with DHS and others as a way to try to encourage the Government to apply this type of model, but to make sure the model is done in such a way that it is not too expensive, too labor intensive, and taking too long to complete. That has certainly been some of the complaints with the common criteria program, is that it does take tremendous amounts of time.

So there is room for a program. I don't think we have hit the ball squarely in the right place in terms of our program, but we have certainly set out a program that is a beginning point that the Government could look at in trying to decide what is a program that is going to meet its needs in laying out the security needs for the Government.

Mr. CLAY. Do you think the Government has taken the security issue as seriously as they should have at this point?

Mr. CARLSON. I think there has been a lot of talk in terms of the importance of security. I think that it has been slow, much slower certainly than I would have anticipated in terms of how quickly the Government has jumped on to some of these ideas, certainly that we have proposed.

I would note this committee had sponsored an effort several years ago, through Congressman Adam Putnam, to kind of bring together Government, private sector, and really to bring together

the user community, which is the community I am most familiar with, and the producer community or the IT community, to try to bridge some of those gaps.

I think we made a lot of progress. Paul Kurtz played a very important role in that effort, as well. But the Government was very slow in terms of picking up on these recommendations and really moving them forward.

I think they have made progress, particularly in the last year, and I noted in my testimony a number of efforts that have been very positive in terms of Greg Garcia being placed as the Assistant Secretary at DHS, the work that the administration did on the Identity Theft Task Force and some of the recommendations that are in there, the work that Karen Evans and others have done at OMB in terms of strengthening Government security programs. So those are all steps in the right direction. But my personal opinion is that it has been much slower than I certainly would have anticipated a few years ago.

Mr. CLAY. Thank you for that response.

Mr. Kurtz, in many of our sensitive or classified programs we use software and applications that have been certified under the National Information Assurance Partnership process. While not perfect, NIAP provides a greater level of software and application assurance for the program. If reducing the number of vulnerabilities in our system is a primary goal, shouldn't we utilize similar certification processes for all agency IT system needs? And others can take a stab at it.

Mr. KURTZ. I would start with maybe a challenge to the premise that NIAP is strong. I think there are enormous issues with the National Information Assurance Partnership. There are terrible inefficiencies, terrible processes associated with that vendors must struggle to go through, and I don't think really at the end of the day agencies get an appreciable increase in security.

That is not to say that the process does not yield some improved security on the part of the software or hardware that goes through the process, but I would not use it as a baseline.

I think there are two points I would try to make. One is I think NIAP needs to be revisited. I think it needs a wholesale review. I know DHS and the Department of Defense engaged in a study of it 3 years ago. I don't think the report has ever seen the light of day. I think Congress should ask for it. I think they should push to make sure that there is a full-scale review of it. And I think we should take a broader view of what is the role of product or software certification in a networked world. It might be, in fact, not as much value as we might hope in that product certification. It is almost a topic for a separate hearing.

You probably asked the wrong guy, because I am going off on it.

Mr. CLAY. Thank you.

Does someone else want to take a stab at it?

Mr. BOND. If I could just real quickly, to followup. And maybe there will be another hearing. But I think certification and accreditation was an important baseline, especially at the time FISMA was passed. But that is a slower boat, if you will, than the threat, and so you could theoretically be in some agency. Veterans have

pointed out you can be 100 percent compliant in terms of your C&A score and still be very vulnerable.

So I think Mr. Lewis testified earlier about really keeping our eye on what is the vulnerability. That is more important than your C&A score.

Mr. CLAY. I appreciate that.

An open question for the entire panel. What would be the potential risks or rewards to the Federal Government if it required its vendors to provide more detailed information concerning the direct evaluation of testing of software code? Couldn't we simply choose the best products if we had this information?

We can start with Mr. Bond.

Mr. BOND. If I can, thank you very much. I think that, again, this is really a question largely about how rapidly the threat evolves. I think it is fair to say that the very best, most assured products could be vulnerable to an unforeseen threat, and the threat evolves rapidly, so assurance of products and sharing as much as you can without giving away some proprietary secret of your product, because it is a competitive market, and I think that is important. But again, you don't want to look in the rear-view mirror as the Government. The very best product today may be vulnerable to some new threat. So I don't want the committee to think that by simply saying make sure that you are as up to date as anybody in the marketplace today, because that may not matter tomorrow.

Mr. CLAY. It is like a moving target.

Mr. BOND. It is.

Mr. CLAY. Thank you.

Mr. KURTZ. Chairman Clay, your question may be focused on source code, the actual software source code?

Mr. CLAY. Yes.

Mr. KURTZ. It is proper to take a look at this issue. I think the good news in this space is just in the past 3 or 4 years a couple of things have happened. One is industry as a whole, the software industry, is getting far more serious about developing good standards of coding, and they are, in fact, seeking to work together to build better standards.

But I think also, equally as important, as typical of the private sector and the free market, enterprises are realizing an opportunity, and they have several new companies out there that recognize the need for code review that can actually analyze code, look for vulnerabilities, and propose mitigation. There are probably five or six that I can name right off the top of my head.

The bottom line of this is I want to think a little bit about mandating some sort of code meeting some spec, some certain level, given the nature of the threats that Mr. Bond has talked about, but I do think it is worthwhile thinking about encouraging the private sector to engage in source code review of some type to use those tools.

I know in the banking and finance industry, because they have a lot of proprietary code, they are using these tools. Others are starting to use these tools. I think we are learning more with each passing day. It is a maturing industry.

There is a move underway in Europe to potentially getting to regulating source code. Incredibly bad idea. Incredibly bad idea that would stymie innovation, stymie research, and good money going into developing new tools for more powerful and more secure code.

Mr. CLAY. Thank you for your opinion.

Mr. Carlson.

Mr. CARLSON. I would add I think the question you really want to be asking is what are the incentives that the Government should put in place to encourage companies to produce the best quality products, in terms of how they are used. As Paul mentioned, my association had done a great deal of work several years ago to put a lot of pressure on the major software companies to make security of greater importance in the development of the products and services. And the industry has certainly responded a great deal and security has become much more of a competitive issue than it was several years ago, and that is a very positive step.

But I think you ought to be careful in terms of going too deep in terms of the specific metrics that you are looking for, but really look for ways to create the incentives that are going to be the drivers for innovation and for companies to really develop these products and services, and then also to find ways that the companies can demonstrate to Government and to private industry how their products are secure, what are the factors that they will use in order to determine whether those products are secure. That would help to secure a certain aspect of the information security equation. It doesn't solve all the problems. It is not a simple solution, but it certainly is a positive step.

Mr. CLAY. Thank you, Mr. Carlson, for reframing the question.

Mr. Lewis.

Mr. LEWIS. Can I add a little bit here? It is always fun to be the last one, and I will say that I agree with Paul that anything the Europeans do we should probably not do. But your question is really: would better software assurance be useful? And the answer is yes. It is, how can the Government push that? What are the incentives?

You might want to think not so much about transparency in the test results or looking at the source code, which is kind of a waste of time, but some idea about what are the practices that companies follow that are paying a lot more attention to security, what are the best practices, and using the acquisitions process to drive that. That is where you have your real leverage in terms of incentives. So there is something of value there.

Mr. CLAY. Thank you so much.

During this panel we have talked about different methods to reduce system vulnerabilities and identify the inherent flaws within IT systems, including the use of software code evaluation. I would like each of you to summarize whether you feel the Federal Government would be an appropriate venue for the development of a new certification model for the evaluation of IT products and software. Specifically, should a new evaluation tool be developed as a voluntary certification program for Federal vendors and agency CIOs to use as a benchmark, or seal of approval, in meeting an agency's security need? If successful and efficient, wouldn't this be-

come a tool that could be widely adopted in the private sector as an alternative to common criteria?

I will begin with you, Mr. Bond.

Mr. BOND. My initial reaction is that the frustration I think we have all had with how slowly information security has moved across the Federal Government is some hint to how quickly they might be able to move to get to the certification that you are looking for, and that we would be better off relying on a faster-moving, more nimble private sector to figure out what is the best there, what is really working in the marketplace, and then quickly adopting the best practices as much as we can.

I would offer another tactical thought, at least for you to consider. We test currently. Under FISMA, we measure whether or not individuals in the agencies are taking courses on awareness about information security. We are not measuring how many of them pass, how many of them retain the information, are they current. We are measuring whether or not they were offered a course.

I think pushing actual measurement of the results down through the Federal enterprise would probably do more.

Mr. CLAY. Thank you for that suggestion.

Mr. Kurtz, please?

Mr. KURTZ. I think I would probably come out where Mr. Lewis is. I think the Government ought to use the power of procurement to encourage vendors to at least talk, to describe what common best practices they are meeting in order to improve software assurance. I think if the Government were to get into the business of establishing that software assurance criteria, it would have a chain effect on R&D and investment in this space.

I do know that industry is working to identify for itself those common standards, and so I would let the marketplace work and then use that in the procurement process to encourage or to incentivize vendors to demonstrate to the Federal Government that they have actually met whatever the private sector standard is for software coding, improved software coding.

Mr. CLAY. Thank you for that response.

Mr. Carlson, please?

Mr. CARLSON. Having some experience developing our own product certification program, I think there are some important caveats to throw out there. One, it is hard work. It takes a lot of time. It is thankless work. You get a lot of push-back from the vendor community in terms of doing it.

I think, in light of Paul's comments in terms of the NIAP process, the common criteria, some of the challenges it is facing, it is probably not the best tool that you can use. It is an important tool, and it would sure be helpful if we had some sort of means by which a company could go through a process to somehow demonstrate that they are as safe as the test could possibly determine. But I think it is important for the Congress and the administration to keep their eyes on the ball in terms of the broader picture, that this is just one tool of many or one factor out of many that really need to be thought about in terms of where do you put the investment to secure an information security program, which is much broader. Encryption is a piece of it. Authentication, access controls,

the vendor management component of it, the training of users and employees—the list is fairly lengthy in terms of how you do it.

Software is an important part of it in terms of that hackers are very good at going through and deciphering where there are vulnerabilities and then exploiting those codes, so that is an important role that software companies have to play. But it needs to be thought of in conjunction of an entire information security program, and whatever program the next version of FISMA is needs to take that into account and to be much more risk based, more performance based in terms of keeping an eye on those risks, because they are going to change and you don't want to be solving yesterday's problem in tomorrow's reality, which could be a very different equation.

Mr. CLAY. Thank you for that assessment.

Mr. Lewis, you can wrap it up.

Mr. LEWIS. Thank you. Thank you, Mr. Chairman.

It is not a bad idea, but I would say the following things: You want a process that is more flexible, certainly more flexible than common criteria, which produced mountains of paper over a very long period of time. You want it to be industry driven. It is not that one company or the other has an answer, but, taken as a whole, they know what the state of play is, and that is probably the best place to go.

You want it to be in partnership with Government, some new way of combining something a little less than regulation, a little more than voluntary effort. You want to look at best practices. I would say stay away from certification. But if you can pull all those in, as Mr. Carlson said, if you can pull all those pieces in what is a thankless process together, you can get some traction out of it.

Thank you.

Mr. CLAY. Thank you. And let me thank the entire panel for your presence here today. You have certainly added something constructive to this discussion. I appreciate it very much.

That concludes this hearing. Thank you all very much.

[Whereupon, at 4:40 p.m., the subcommittees were adjourned.]

○