

# THE STATE OF FEDERAL INFORMATION SECURITY

---

---

## HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,  
ORGANIZATION, AND PROCUREMENT

OF THE

COMMITTEE ON OVERSIGHT  
AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

MAY 19, 2009

**Serial No. 111-52**

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

57-125 PDF

WASHINGTON : 2010

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://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 OVERSIGHT AND GOVERNMENT REFORM

EDOLPHUS TOWNS, New York, *Chairman*

PAUL E. KANJORSKI, Pennsylvania  
CAROLYN B. MALONEY, New York  
ELIJAH E. CUMMINGS, Maryland  
DENNIS J. KUCINICH, Ohio  
JOHN F. TIERNEY, Massachusetts  
WM. LACY CLAY, Missouri  
DIANE E. WATSON, California  
STEPHEN F. LYNCH, Massachusetts  
JIM COOPER, Tennessee  
GERALD E. CONNOLLY, Virginia  
MIKE QUIGLEY, Illinois  
MARCY KAPTUR, Ohio  
ELEANOR HOLMES NORTON, District of  
Columbia  
PATRICK J. KENNEDY, Rhode Island  
DANNY K. DAVIS, Illinois  
CHRIS VAN HOLLEN, Maryland  
HENRY CUELLAR, Texas  
PAUL W. HODES, New Hampshire  
CHRISTOPHER S. MURPHY, Connecticut  
PETER WELCH, Vermont  
BILL FOSTER, Illinois  
JACKIE SPEIER, California  
STEVE DRIEHAUS, Ohio

DARRELL E. ISSA, California  
DAN BURTON, Indiana  
JOHN M. McHUGH, New York  
JOHN L. MICA, Florida  
MARK E. SOUDER, Indiana  
TODD RUSSELL PLATTS, Pennsylvania  
JOHN J. DUNCAN, JR., Tennessee  
MICHAEL R. TURNER, Ohio  
LYNN A. WESTMORELAND, Georgia  
PATRICK T. McHENRY, North Carolina  
BRIAN P. BILBRAY, California  
JIM JORDAN, Ohio  
JEFF FLAKE, Arizona  
JEFF FORTENBERRY, Nebraska  
JASON CHAFFETZ, Utah  
AARON SCHOCK, Illinois

RON STROMAN, *Staff Director*  
MICHAEL MCCARTHY, *Deputy Staff Director*  
CARLA HULTBERG, *Chief Clerk*  
LARRY BRADY, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

DIANE E. WATSON, California, *Chairman*

PAUL E. KANJORSKI, Pennsylvania  
JIM COOPER, Tennessee  
GERALD E. CONNOLLY, Virginia  
HENRY CUELLAR, Texas  
JACKIE SPEIER, California  
PAUL W. HODES, New Hampshire  
CHRISTOPHER S. MURPHY, Connecticut

BRIAN P. BILBRAY, California  
AARON SCHOCK, Illinois  
JOHN J. DUNCAN, JR., Tennessee  
JEFF FLAKE, Arizona

# CONTENTS

	Page
Hearing held on May 19, 2009 .....	1
Statement of:	
Kundra, Vivek, Federal Chief Information Officer, Administrator for Electronic Government and Information Technology, Office of Management and Budget; Gregory Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office; Jacquelyn Patillo, Acting Chief Information Officer, U.S. Department of Transportation; Margaret H. Graves, Acting Chief Information Officer, U.S. Department of Homeland Security; Samuel Chun, Director, Cyber Security Practice, EDS U.S. public sector, a Hewlett-Packard Co.; and M.J. Shoer, president and virtual chief technology officer, Jenaly Technology Group, Inc. ....	5
Chun, Samuel .....	47
Graves, Margaret H. ....	36
Kundra, Vivek .....	5
Patillo, Jacquelyn .....	28
Shoer, M.J. ....	56
Wilshusen, Gregory .....	10
Letters, statements, etc., submitted for the record by:	
Chun, Samuel, Director, Cyber Security Practice, EDS U.S. public sector, a Hewlett-Packard Co., prepared statement of .....	49
Graves, Margaret H., Acting Chief Information Officer, U.S. Department of Homeland Security, prepared statement of .....	38
Kundra, Vivek, Federal Chief Information Officer, Administrator for Electronic Government and Information Technology, Office of Management and Budget, prepared statement of .....	8
Patillo, Jacquelyn, Acting Chief Information Officer, U.S. Department of Transportation, prepared statement of .....	29
Shoer, M.J., president and virtual chief technology officer, Jenaly Technology Group, Inc., prepared statement of .....	59
Wilshusen, Gregory, Director, Information Security Issues, U.S. Government Accountability Office, prepared statement of .....	12



# THE STATE OF FEDERAL INFORMATION SECURITY

TUESDAY, MAY 19, 2009

HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,  
ORGANIZATION, AND PROCUREMENT,  
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,  
*Washington, DC.*

The subcommittee met, pursuant to notice, at 9:25 a.m., in room 2247, Rayburn House Office Building, Hon. Diane Watson (chairwoman of the subcommittee) presiding.

Present: Representatives Watson, Bilbray, Connolly, and Duncan.

Staff present: Bert Hammond, staff director; Valerie Van Buren, clerk; Adam Bordes and Deborah Mack, professional staff; Dan Blankenberg, minority chief counsel for policy; Adam Fromm, minority director of outreach and senior advisor; Kurt Bardella, minority chief clerk and Member liaison; John Ohly, minority professional staff member; and Katy Rother, minority staff assistant.

Ms. WATSON. The Subcommittee on Government Management, Organization, and Procurement of the Committee on Oversight and Government Reform will now come to order.

Welcome. Today's hearing will review the Federal Information Security Management Act [FISMA] of 2002, and agencies' efforts to improve the security, integrity and reliability of the Federal Government's information systems. In addition, the hearing will seek to learn more about the new administration's strategic objectives for achieving FISMA compliance, as well as the scope for improving how agencies mitigate the number of risks facing their systems.

Without objection, the Chair and ranking minority member will have 5 minutes to make opening statements, followed by opening statements not to exceed 3 minutes by any Member who seeks recognition.

Without objection, Members and witnesses may have 5 administrative days to submit a written statement of extraneous materials for the record.

I wish all of you a good morning. And welcome to today's subcommittee hearing on Federal Information Security and Review of Agency Efforts to Comply with the Federal Information Security Management Act. I welcome our distinguished witnesses and look forward to hearing the testimony.

Since FISMA was enacted in 2002, the Federal Government has made significant progress in securing its key network and information technology access. That said, FISMA only [inaudible] informa-

tion [inaudible] and [inaudible] are only required to read one chapter of a book. Although FISMA does require [inaudible] on how agencies are covering their information security bases, it does nothing to tell us about the current vulnerability landscape or how the cyber-threats may be changing. If FISMA is to become a more useful tool for countering cyber-threats, it must require agencies to utilize better testing, monitoring and performance measures for determining what our true cybersecurity posture is.

According to the GAO, 20 out of 24 agencies have been identified as having either material weaknesses or material deficiencies in their information security controls. In other words, these agencies are lacking key controls that are necessary for maintaining a sound security program. The failure to establish these controls leaves agencies vulnerable to significant data breaches and disruptions to key critical infrastructure and potential compromises of our national security. These weaknesses are widespread within key programs of both the Department of Transportation and the Department of Homeland Security and must be remedied in order to ensure the proper functioning of our Government's IP assets.

Today, I am hoping our agency witnesses will tell us what changes are underway to remedy the problems identified through the work of GAO and the IG community. Furthermore, I want our new Federal CIO, Mr. Kundra, to tell us what this plan or what his plan objectives are for strengthening FISMA and how the soon to be released 60-day White House cyber-review will impact the use or relevance of FISMA going forward.

Last, I would like to hear our panelists' specific recommendations for legislation to develop a harmonized framework for organizing and for coordinating Government-wide information security policies and practices.

Once again, I would like to thank our panel for joining us today and look forward to their testimony.

Now, the ranking member, Mr. Bilbray.

Mr. BILBRAY. Thank you, Madam Chairman. I appreciate this hearing.

Let me just first of all ask that my written statement be entered into the record.

Ms. WATSON. Without objection, so ordered.

Mr. BILBRAY. Madam Chair [remarks off mic].

Let me say that [inaudible] San Diego [inaudible].

[Technical adjustment.]

Mr. BILBRAY. Thank you, Madam Chair.

Let me just say that one of my biggest concerns after being briefed by a lot of my experts in San Diego, which is a bit of a hot bed of information services, as everybody knows, besides QualCom and many other secret hideaway, high tech firms, but this is really an underestimated threat to our national security in a lot of ways. And it is not just within our military, it is not just within our own Government operations, it is national. Every private sector, every public sector, has this threat hanging over our heads.

I think one thing we learned from 9/11 is the good old comment that we didn't know, or we didn't think we needed to do that much is not acceptable any more. Frankly, if we can't maintain some kind of security over our systems at the Federal Government, we

are going to be hard pressed to try to figure out how to coordinate the private sector, and even ask the private sector to do more, when it appears that out of 24 major departments, we have 23 that have found deficiencies.

I just think the challenge here is for us to lead through example and really try to get down to the root cause of these deficiencies and how we can modify our operations to avoid them in the future. And maybe, just maybe, we can do something that is never done very much in this town, and that is lead through example for the private sector and show them how to address this challenge.

So I look forward to the hearing. I look forward to the opportunities to dialog with the witnesses and with fellow members of this committee, because I think it is something that we are going to have to spend a lot more time and effort addressing to make sure that we don't live to see the day when there is a 9/11, a cyber-version of 9/11 somewhere over the horizon.

Thank you very much for the hearing again.

Ms. WATSON. Thank you, Mr. Bilbray.

I now yield to Mr. Connolly.

Mr. CONNOLLY. Thank you, Chairwoman Watson, for holding this timely hearing, which complements our recent hearing on cybersecurity. This is an exciting time to be pursuing reforms in Federal information security programs. With Aneesh Chopra and Vivek Kundra as newly appointed Chief Technology and Chief Information Officers, we have extraordinary expertise at the executive level.

First, we should acknowledge the many Federal employees who have done a good job implementing the Federal Information Security Management Act [FISMA] of 2002. Since 2005, most Federal agencies have significantly improved implementation of contingency plans and completed inventories. In the last 7 years we have made significant progress, even as information security threats have grown.

However, there is still room for improvement. For example, the number of employees receiving specialized security training declined between fiscal year 2007 and fiscal year 2008. The GAO report also notes that FISMA requires security awareness training for contractors as well as agency personnel. At our May 5th hearing on cybersecurity, we learned that many security breaches occurred through contractor information systems. Perhaps metrics should take breaches into account. Since more than 90 percent of personnel and contractors are receiving security awareness training, perhaps the effectiveness and frequency of the training needs to be reexamined.

In their prepared testimony for today, both CIO Vivek Kundra and EDS employee Samuel Chun note that some agencies may be focused more on compliance with FISMA than performance of their security systems. Moreover, they note that reporting requirements under FISMA could be streamlined. I look forward to learning more about how FISMA could be reformed to emphasize performance and minimize unnecessary paperwork.

Thank you again, Chairwoman Watson, for holding this hearing. I appreciate the work this subcommittee is conducting to enhance

information and cybersecurity in the Federal Government, and look forward to the testimony at today's hearing.

Ms. WATSON. Thank you, Mr. Connolly.

Mr. Duncan.

Mr. DUNCAN. Thank you very much, Madam Chairwoman.

I pushed this button but—

Ms. WATSON. Yes, I know. We are having trouble. [Remarks off mic.] [Laughter.]

Mr. DUNCAN. I don't really have a formal statement anyway. I do thank you for calling this hearing. I do sometimes wonder if true cybersecurity is possible. I remember several years ago coming back from lunch in my district one time and I heard on the CBS national radio news that computer hackers had gotten into the top secret files of the Pentagon hundreds of times, some report had just come out. And then I remember reading a few years ago a front page story in the Washington Post where a 12 year old boy in California had opened the floodgates at the Hoover Dam, a great distance away, hundreds of miles away, by hacking into the system.

So I don't know, it seems to me that it may be possible we started out controlling computers and now they control us. Everybody, or especially young people, worship the technology today and are addicted to it. But it seems to me that this is a serious problem. We've almost done away with any kind of privacy or secrecy in this country because it seems that anybody can find out anything that they want to, and that includes people who wish to do us harm from other countries.

So this is a serious problem and I am a little skeptical as to whether we can actually do what needs to be done. But I do think it is good that you called this hearing. Thank you very much.

Ms. WATSON. Thank you, and if there is no further testimony, I would like now to go to the panel. Would you all stand, please?

It is the policy of the Committee on Oversight and Government Reform to swear in all witnesses before they testify. And I would like to ask all of you to stand and raise your right hands.

[Witnesses sworn.]

Ms. WATSON. OK, let the record reflect that the witnesses answered in the affirmative.

I would like to now introduce the panelists. First, we have Vivek Kundra, the Chief Information Officer at the Office of Management and Budget. Mr. Kundra was appointed as the first Federal CIO of the United States by President Obama in March 2009. In this capacity, he directs the policy and strategic planning of Federal information technology investments and is responsible for oversight of Federal technological spending.

Prior to joining the Obama administration, Mr. Kundra served in Mayor Fenty's cabinet as the chief technology officer for the District of Columbia and Governor Kane's cabinet as assistant secretary of commerce and technology for the Commonwealth of Virginia.

Mr. Gregory Wilshusen serves as the Director of Information Security Issues at GAO. His work involves examining Federal information security practices and trends at Federal agencies. He is GAO's leading expert on FISMA implementation.

Ms. Jacquelyn Patillo is the Acting Chief Information Officer at the Department of Transportation. And at DOT, Ms. Patillo serves as the principal advisor to the Department's CIO on matters involving information resources and information services management. Prior to her current role, Ms. Patillo served as the Deputy CIO for DOT and as Chief Information officer at the National Highway Traffic Safety Administration.

Ms. Margaret Graves is the Acting Chief Information Officer at the Department of Homeland Security. There she oversees an IT portfolio of \$5.4 billion in programs, as well as the operations of the Office of the Chief Information Officer, which covers the financial or functional areas of applied technologies, enterprise architecture, data manager, IT security infrastructure operations, IT accessibility, budget and acquisition.

Mr. Samuel Chun is the director for the Cyber Security Practice for the U.S. public sector at EDS, a division of Hewlett-Packard. And there he is responsible for the strategy portfolio development in industry messaging of all cyber security solutions for EDS' U.S. public sector clients.

And Mr. M.J. Shoer is the president of Jenaly Technology Group, Inc. He is here today on behalf of the Computing Technology Industry Association. Founded by Mr. Shoer in 1997, the Jenaly Technology Group provides outsourced IP services to small business throughout New Hampshire.

I would also like to recognize his daughter, Hannah, who traveled with him to today's hearing.

I would like to say again, welcome to all of you. I ask that each of the witnesses now give a brief summary of their testimony and to keep the summary under 5 minutes if possible. Your complete statement will be included in the hearing record.

Mr. Kundra, would you please proceed?

**STATEMENTS OF VIVEK KUNDRA, FEDERAL CHIEF INFORMATION OFFICER, ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET; GREGORY WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; JACQUELYN PATILLO, ACTING CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF TRANSPORTATION; MARGARET H. GRAVES, ACTING CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY; SAMUEL CHUN, DIRECTOR, CYBER SECURITY PRACTICE, EDS U.S. PUBLIC SECTOR, A HEWLETT-PACKARD COMPANY; AND M.J. SHOER, PRESIDENT AND VIRTUAL CHIEF TECHNOLOGY OFFICER, JENALY TECHNOLOGY GROUP, INC.**

#### **STATEMENT OF VIVEK KUNDRA**

Mr. KUNDRA. Good morning, Chairwoman Watson, Ranking Member Bilbray, Congressman Connolly and Congressman Duncan. Thank you for the opportunity to testify on the state of Federal information security.

The security of Federal information systems is a major concern for this administration. Our Nation's security and economic pros-

perity depend on the stability and integrity of our Federal communications systems and infrastructure. Safeguarding these important interests will require balanced a decisionmaking process that integrates and harmonizes our national and economic security objectives with our privacy rights, civil liberties and open government.

As a first step, the president has directed a 60-day review of cybersecurity policies and efforts throughout the Federal Government. OMB is working closely, along with other agencies, with Acting Senior Director Melissa Hathaway of the National Security Council and her team on this review.

During the last several decades, the United States and the world have been moving from a paper-based world to a digital world. Advances in technology are fundamentally changing the way business is done, increasing productivity and providing the American people easy access to services that previously were structurally impossible to deliver electronically.

Essential to these new capabilities is the presence of communications networks that security carry sensitive information. Yet, as we have unleashed new transactions over this network, a new class of risks has emerged. The American people need to trust that the information they are submitting to or receiving from the Government is accurate, reliable and secure.

However, recent successful breaches at the Federal Aviation Administration and at the vendor that hosts USAjobs.gov demonstrate that the current Federal information security posture is not what the American people have a right to expect. The Federal Information Security Management Act has been in place for 7 years. It has raised the level off awareness in agencies and in the country at large, but we are not where we need to be.

In our initial review of information security, the following things have surfaced. One, the performance information currently collected under FISMA does not reflect the security posture of Federal agencies. Two, the process used to collect the information is cumbersome, labor-intensive and takes away time from meaningful analysis. And three, the Federal community is focused too much on compliance and not enough on outcomes.

While the current reporting metrics may have made sense when FISMA was enacted, they are largely compliance-based. They are trailing, rather than leading indicators. We need metrics that give us insight into agency security postures and possible vulnerabilities on an ongoing basis.

To evaluate new metrics, we are taking a collaborative approach. We are working with a community of Federal agency Chief Information Officers, Chief Information Security Officers, Inspector Generals and the National Institute of Standards and Technology to consider more effective security measures, ones that show current status and are predictive in nature. In addition, we are reaching out to a broad array of organizations, across the public and private sectors and academia.

Today, agencies and IGs are heavily focused on compliance. The creation of a secure, transparent, collaborative environment requires a risk-based approach. We will never achieve our security goals through compliance alone, because security threats are fluid and constantly changing. Each new technology, new employee and

new program represents potential for additional security weaknesses. Agencies need to adopt a risk-based approach to security to look at activities, people and programs on an ongoing basis.

The administration is committed to creating a trusted, secure Federal computing environment that makes information transparent to the American people while protecting privacy and confidentiality. While the actions I have spoken about here will assist in creating that environment, they alone are not enough. A secure, trusted computing environment in the Federal Government is the responsibility of everyone involved, from the agency heads to those charged with oversight. It entails employees, contractors and the American people working together to create a culture of vigilance and security that enable us to continue and efficiently leverage the power of technology.

Thank you for the opportunity to testify on this very important issue, and I look forward to your questions.

[The prepared statement of Mr. Kundra follows:]

**STATEMENT OF VIVEK KUNDRA  
FEDERAL CHIEF INFORMATION OFFICER,  
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND  
INFORMATION TECHNOLOGY  
OFFICE OF MANAGEMENT AND BUDGET**

**BEFORE THE  
HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM  
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND  
PROCUREMENT**

**May 19, 2009**

Good morning, Chairwoman Watson, Ranking Member Bilbray, and members of the Subcommittee. Thank you for the opportunity to testify on the state of Federal information security.

The security of Federal information systems is a major concern of this Administration. Our nation's security and economic prosperity depend on the stability and integrity of our Federal communications and information infrastructure. Safeguarding these important interests will require balanced decision-making that integrates and harmonizes our national and economic security objectives with our privacy rights, civil liberties, and open government. As a first step, the President has directed a 60-day review of cybersecurity policies and efforts throughout the government. OMB is working closely along with other agencies with Acting Senior Director Melissa Hathaway of the National Security Council and her team on this review.

During the last twenty years, the United States and the world have been moving from a paper-based world to a digital world. Advances in technology are fundamentally changing the way business is done, increasing productivity, and providing the American people easy access to services in ways previously structurally impossible.

Essential to these new capabilities is the presence of communications networks that securely carry sensitive information. Yet, as we have unleashed new transactions over this network, a new class of risks has emerged. The American people need to trust that the information they are submitting to or receiving from the government is accurate, reliable, and secure.

However, recent successful breaches at the Federal Aviation Administration and at the vendor that hosts USAjobs.gov demonstrate that the current state of information security at Federal agencies is not what the American people have the right to expect. The Federal Information Security Management Act (FISMA) has been in place for 7 years. It has raised the level of awareness in the agencies and in the country at large, but we are not where we need to be.

In our initial review of information security issues, the following issues have surfaced:

- The performance information currently collected under FISMA does not fully reflect the security posture of Federal agencies;
- The processes used to collect the information are cumbersome, labor-intensive, and take time away from meaningful analysis, and;
- The Federal community is focused on compliance, not outcomes.

While the current reporting metrics may have made sense when FISMA was enacted, they are largely compliance based. They are trailing, rather than leading, indicators. We need metrics that give insight into agencies' security postures and possible vulnerabilities on an on-going basis.

To evaluate new metrics, we are taking a collaborative approach. We are working with the community of Federal agency Chief Information Officers and Chief Information Security Officers, as well as the Inspectors General and the National Institute of Standards and Technology, to consider more effective security performance metrics -- ones that show current status and are predictive in nature. In addition, we are reaching out to a broad array of organizations, across the public and private sectors and academia.

Today, agencies and IGs are heavily focused on compliance. The creation of a secure, transparent, collaborative environment requires a risk-based approach. We will never achieve our security goals through compliance alone because security threats are fluid and constantly changing. Each new technology, new employee, and new program represents the potential for additional security weakness. Agencies need to adopt a risk-based approach to security, to look at activities, people and programs on an on-going basis.

The Administration is committed to creating a trusted, secure Federal computing environment that makes information transparent to the American people while protecting privacy and confidentiality. While the actions I have spoken about here will assist in creating that environment, they alone are not enough. A secure, trusted computing environment in the Federal Government is the responsibility of everyone involved from the agency heads to those charged with oversight. It entails employees, contractors, and the American people working together to create a culture of vigilance and security to enable us to continue to efficiently leverage the power of technology.

Thank you for this opportunity to testify on this important issue, and I look forward to your questions.

Ms. WATSON. Thank you, Mr. Kundra.  
Mr. Wilshusen, you may proceed.

#### STATEMENT OF GREGORY WILSHUSEN

Mr. WILSHUSEN. Good morning, Chairwoman Watson, Ranking Member Bilbray and members of the subcommittee.

Thank you for the opportunity to participate in today's hearing on the state of Federal information security. Information security is a critical consideration for any organization that depends on computerized systems and networks to carry out its mission or business. It is especially important for Federal agencies where maintaining the public trust is Essential.

Without proper safeguards, Federal systems and networks are vulnerable to intrusions by individuals and groups with malicious intent who could potentially obtain and manipulate sensitive data, commit fraud, disrupt operations and launch attacks against other computer systems. The Federal Information Security Management Act [FISMA], was enacted in part to provide a comprehensive framework for assuring the effectiveness of information security controls over information resources that support Federal operations and assets.

Madam Chairwoman, 2 weeks ago I testified before you and this subcommittee about the growing and evolving nature of cyber threats upon our abilities and the challenges that place Federal systems and operations at risk. Today, I will discuss agencies' progress in performing key information security control activities, the effectiveness of information security at Federal agencies, and opportunities to bolster security.

In fiscal year 2008, Federal Government reported improved information security performance relative to most of the key performance metrics established by OMB. Although the percentage of employees with significant security responsibilities who receive specialized training decreased significantly, increases were reported in the number of employees and contractors who received security awareness training, the percentage of systems with test to contingency plans and the percentage of systems that were certified and accredited.

Despite reported progress, major Federal agencies continue to experience significant control deficiencies. Most agencies did not implement controls that sufficiently prevent, limit or detect access to computer network systems or information.

Moreover, agencies do not always configure networks, devices and services to prevent unauthorized access and assure system integrity, patch key servers and workstations in a timely manner, and maintain complete continuity of operations plans for key information systems. An underlying cause for these weaknesses is that most agencies have not fully or effectively implemented elements of agency-wide information security programs mandated by FISMA.

These factors continue to place Federal assets at risk of inadvertent or deliberate mis-use, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure and critical operations at risk of disruption. Accordingly, GAO has again designated Federal information secu-

rity as a Government-wide high risk area in its 2009 high risk report to the Congress.

Nevertheless, opportunities exist to bolster Federal information security. Federal agencies could implement the hundreds of recommendations made by GAO and agency IGs to resolve previously reported control deficiencies in information security program shortfalls.

In addition, the White House, OMB and other Federal agencies have continued or launched several Government-wide initiatives that are intended to improve information security over systems and information. For example, in January 2008, the White House launched a series of initiatives collectively known as the Comprehensive National Cybersecurity Initiative, aimed primarily at improving the Department of Homeland Security and other Federal agencies' efforts to protect against intrusion attempts and anticipate future threats.

In summary, although Federal agencies report performing key control activities for an increasing percentage of their systems, persistent weaknesses in agency information security continues to threaten the confidentiality, integrity and availability of Federal systems and information. To help address these and other challenges, sustained commitment, effective oversight and improvements to the National Cybersecurity Strategy are needed to strengthen Federal information security.

Chairwoman Watson, this concludes my opening statement. I would be happy to answer your questions at the appropriate time.

[The prepared statement of Mr. Wilshusen follows:]

---

United States Government Accountability Office

---



Testimony Before the  
Subcommittee on Government Management,  
Organization, and Procurement,  
Committee on Oversight and Government Reform,  
U.S. House of Representatives

---

For Release on Delivery  
Expected at 9:00 a.m. EDT  
May 19, 2009

## INFORMATION SECURITY

# Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist



May 19, 2009

G A O  
Accountability · Integrity · Reliability

## Highlights

Highlights of GAO-09-701T, a testimony before the House Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, House of Representatives

### Why GAO Did This Study

Without proper safeguards, federal agencies' computer systems are vulnerable to intrusions by individuals and groups who have malicious intentions and can obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. Concerned by reports of significant weaknesses in federal systems, Congress passed the Federal Information Security Management Act (FISMA), which permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies.

GAO was asked to testify on its draft report on (1) the adequacy and effectiveness of federal agencies' information security policies and practices and (2) their implementation of FISMA requirements. To prepare for this testimony, GAO summarized its draft report where it analyzed agency, inspectors general, Office of Management and Budget (OMB), congressional, and GAO reports on information security.

### What GAO Recommends

In its draft report, GAO is recommending that the Director of OMB take several actions, including revising guidance.

View GAO-09-701T or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

## INFORMATION SECURITY

### Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist

#### What GAO Found

Significant weaknesses in information security policies and practices expose sensitive data to significant risk, as illustrated by recent incidents at various agencies. GAO's audits and reviews by inspectors general note significant information security control deficiencies that place agency operations and assets at risk. In their fiscal year 2008 performance and accountability reports, 20 of 24 major agencies noted that the information system controls over their financial systems and information were either a significant deficiency or a material weakness. In addition, over the last several years, most agencies have not implemented controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements for an agencywide information security program, as required by FISMA. Twenty-three of the 24 major federal agencies had weaknesses in their agencywide information security programs.

Federal agencies reported increased compliance in implementing key information security control activities for fiscal year 2008; however, inspectors general at several agencies noted shortcomings with agencies' implementation of information security requirements. For fiscal year 2008 reporting, agencies reported higher levels of FISMA implementation for most information security metrics and lower levels for others. Increases were reported in the number and percentage of employees and contractors receiving security awareness training, the number and percentage of systems with tested contingency plans, and the number and percentage of systems that were certified and accredited. However, the number and percentage of employees who had significant security responsibilities and had received specialized training decreased significantly and the number and percentage of systems that had been tested and evaluated at least annually decreased slightly. In addition, the current reporting instructions do not request inspectors general to report on agencies' effectiveness of key activities and did not always provide them with clear guidance for annual reporting. This information could be useful in determining whether agencies are effectively implementing information security policies, procedures, and practices. Without such information, Congress may not be fully informed about the state of federal information security.

---

Chairwoman Watson and Members of the Subcommittee:

Thank you for inviting me to discuss our work on federal agencies' implementation of information security policies and practices under the Federal Information Security Management Act of 2002 (FISMA).<sup>1</sup> Information security is a critical consideration for any federal department or agency, where information systems and computer networks are used to carry out its mission and where maintaining the public's trust is essential. The need for a vigilant approach to information security is demonstrated by the increase in reports of security incidents, the wide availability of hacking tools, and steady advances in the sophistication and effectiveness of attack technology.

Without proper safeguards, federal agencies' computer systems are vulnerable to intrusions by individuals and groups with malicious intentions who can obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. The risks to federal systems are well-founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology. Over the past few years, the 24 major federal agencies<sup>2</sup> have reported numerous security incidents in which sensitive information has been lost or stolen, including personally identifiable information, which has exposed millions of Americans to the loss of privacy, identity theft, and other financial crimes.

---

<sup>1</sup>FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

<sup>2</sup>The 24 major departments and agencies (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.

---

Concerned by reports of significant weaknesses in federal systems, Congress passed FISMA in 2002, which permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies. Six years after FISMA was enacted, we continue to report that poor information security is a widespread problem with potentially devastating consequences. Moreover, since 1997, we have identified information security as a governmentwide high-risk issue in our biennial reports to Congress.<sup>3</sup>

In my testimony today, I will summarize the results of our review of (1) the adequacy and effectiveness of federal agencies' information security policies and practices and (2) agencies' implementation of FISMA. We currently have a draft report providing additional detail on that review that we will be finalizing and issuing publicly at a later date. In conducting our review, we analyzed agency, inspector general, Office of Management and Budget (OMB), congressional, and our reports on information security. We conducted the review from December 2008 to May 2009 in the Washington, D.C., area in accordance with generally accepted government auditing standards.

After a brief summary of the laws and guidance currently in place, my remarks will focus on the results of our review.

---

## Background

FISMA sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Its framework creates a cycle of risk management activities necessary for an effective security program; these activities are similar to the principles noted in our study of the risk management activities of leading private sector organizations<sup>4</sup>—assessing risk, establishing a central management focal point, implementing appropriate policies

---

<sup>3</sup>Most recently, GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

<sup>4</sup>GAO, *Executive Guide: Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

---

and procedures, promoting awareness, and monitoring and evaluating policy and control effectiveness. In order to ensure the implementation of this framework, FISMA assigns specific responsibilities to agency heads, chief information officers, inspectors general, and the National Institute for Science and Technology (NIST). It also assigns responsibilities to OMB, which include developing and overseeing the implementation of policies, principles, standards, and guidelines on information security and reviewing, at least annually, and approving or disapproving, agency information security programs.

---

#### Federal Law and Policy Established Federal Information Security Requirements

FISMA requires each agency, including agencies with national security systems, to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Specifically, FISMA requires information security programs to include, among other things

- periodic assessments of the risk that could result from the compromise of information or information systems;
- risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- security awareness training for agency personnel, including contractors;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies;

- 
- procedures for detecting, reporting, and responding to security incidents;
  - plans and procedures to ensure continuity of operations; and
  - an annually updated inventory of major information systems operated by the agency or under its control.

FISMA also requires each agency to report annually to OMB, selected congressional committees, and the comptroller general on the adequacy of its information security policies, procedures, practices, and compliance with requirements. In addition, agency heads are required to report annually the results of their independent evaluations to OMB, except to the extent that an evaluation pertains to a national security system; then only a summary and assessment of that portion of the evaluation needs to be reported to OMB.

NIST, agency inspectors general, and OMB also play key roles under FISMA. NIST, for example, is required to provide standards and guidance to agencies on information security. In addition, NIST is tasked with developing a definition of and guidelines for detection and handling of information security incidents as well as guidelines developed in conjunction with the Department of Defense and the National Security Agency for identifying an information system as a national security system. NIST has issued guidance through its FISMA Implementation Project and has expanded its work through other security activities. In addition, NIST's computer security division issued its 2008 annual report, as mandated by FISMA. Agency inspectors general are required to perform an independent annual evaluation of the agency's information security program and practices. These reviews should include testing of information security procedures policies and practices for a representative subset of agency systems, as well as an assessment of compliance with FISMA and any related information security policies, procedures, standards, and guidelines.

FISMA also requires OMB to develop policies, principles, standards, and guidelines on information security and is required to report annually to Congress on agency compliance with the requirements

---

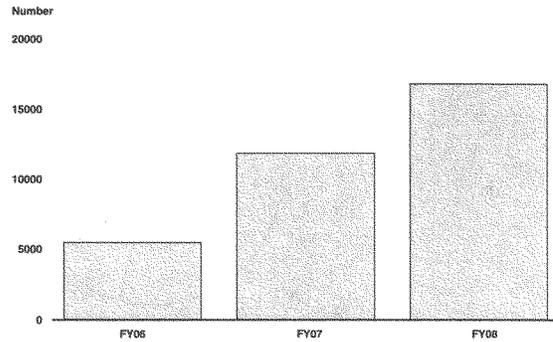
of the act. OMB has provided instructions to federal agencies and their inspectors general for preparing annual FISMA reports. OMB's reporting instructions focus on performance metrics related to the performance of key control activities such as developing a complete inventory of major information systems, providing security training to personnel, testing and evaluating security controls, testing contingency plans, and certifying and accrediting systems.

---

### **Weaknesses in Information Security Controls Place Sensitive Information at Risk**

Significant weaknesses in information security policies and practices expose sensitive data to significant risk, as illustrated by recent incidents at various agencies. 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. When incidents occur, agencies are to notify the federal information security incident center—US-Computer Emergency Readiness Team (US-CERT). As shown in figure 1, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 3 years, increasing from 5,503 incidents reported in fiscal year 2006 to 16,843 incidents in fiscal year 2008 (about a 206 percent increase).

**Figure 1: Incidents Reported to US-CERT, FY 2006 — FY 2008**

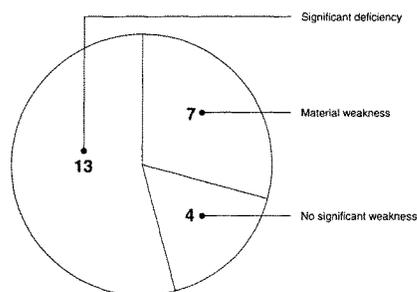


Source: GAO analysis of US-CERT data.

Reviews at federal agencies continue to highlight deficiencies in their implementation of security policies and procedures. In their fiscal year 2008 performance and accountability reports, 20 of 24 major agencies noted that their information system controls over their financial systems and information were either a material weakness or a significant deficiency<sup>5</sup> (see fig. 2).

<sup>5</sup>A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

**Figure 2: Number of Major Agencies Reporting Significant Deficiencies in Information Security**



Source: GAO analysis of agency performance and accountability reports for FY2008.

Agency inspectors general have also reported weaknesses in information security, with 22 of 24 identifying information security as a “major management challenge” for their agency.<sup>6</sup>

Over the last several years, most agencies have not implemented controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. For example, our analysis of inspector general, agency, and our own reports reveals that agencies did not have adequate controls in place to ensure that only authorized individuals could access or manipulate data on their systems and networks. Weaknesses were reported in such controls at 23 of 24 major agencies for fiscal year 2008. 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

<sup>6</sup>The Reports Consolidation Act of 2000, Pub. L. No. 106-531, 114 Stat. 2537 (Nov. 22, 2000), requires inspectors general to include in their agencies’ performance and accountability reports a statement that summarizes what they consider to be the most serious management and performance challenges facing their agencies and briefly assesses their agencies’ progress in addressing those challenges. 31 U.S.C. § 3516(d).

---

encryption to protect sensitive data on networks and portable devices, and (5) log, audit, and monitor security-relevant events. At least nine agencies also lacked effective controls to restrict physical access to information assets. We have previously reported that many of the data losses occurring 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.

In addition, agencies did not always configure network devices and services to prevent unauthorized access and ensure system integrity, patch key servers and workstations in a timely manner, or segregate incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction. Furthermore, agencies did not always ensure that continuity of operations plans contained all essential information necessary to restore services in a timely manner. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of information.

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements for an agencywide information security program, as required by FISMA. An agencywide security program, as 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. Twenty-three of the 24 major federal agencies had weaknesses in their agencywide information security programs. Due to the persistent nature of information security vulnerabilities and the associated risks, we continue to designate information security as a governmentwide high-risk issue in our most recent biennial report to Congress;<sup>7</sup> a designation we have made in each report since 1997.

---

<sup>7</sup>GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

---

---

### Enhancements Can Be Made to Strengthen Federal Information Security

Over the past several years, we and agency inspectors general have made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls. For example, we recommended that agencies correct specific information security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, and contingency planning. We have also recommended that agencies fully implement comprehensive, agencywide information security programs by correcting shortcomings in risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. The effective implementation of these recommendations will strengthen the security posture at these agencies.

In addition, the White House, OMB, and some federal agencies have continued or launched several governmentwide initiatives that are intended to enhance information security at federal agencies. They include the Comprehensive National Cyber Security Initiative, the Information Systems Security Line of Business, the Federal Desktop Core Configuration, SmartBUY, and the Trusted Internet Connections Initiative. We currently have ongoing work that addresses the status, planning, and implementation efforts of several of these initiatives.

---

### Agencies Continue to Report Progress in Implementing Requirements

Federal agencies reported increased compliance in implementing key information security control activities for fiscal year 2008; however, inspectors general at several agencies noted shortcomings with agencies' implementation of information security requirements. OMB also reported that agencies' were increasingly performing key

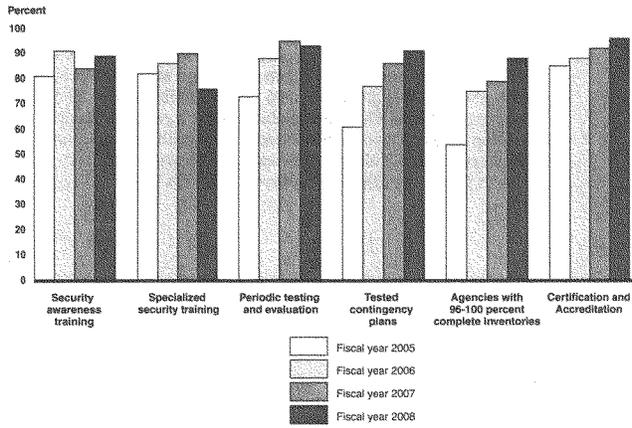
---

activities. Specifically, agencies reported increases in the number and percentage of systems that had been certified and accredited,<sup>8</sup> the number and percentage of employees and contractors receiving security awareness training, and the number and percentage of systems with tested contingency plans. However, the number and percentage of systems that had been tested and evaluated at least annually decreased slightly (from 95 percent in fiscal year 2007 to 93 percent in fiscal year 2008) and the number and percentage of employees who had significant security responsibilities and had received specialized training decreased significantly (from 90 percent in fiscal year 2007 to 76 percent in 2008). (See fig 3.)

---

<sup>8</sup>Certification is a comprehensive assessment of management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision to authorize operation of an information system and to explicitly accept the risk to agency operations based on implementation of controls.

**Figure 3: Selected Performance Metrics for Agency Systems**



Source: GAO analysis of IG and agency data.

**Most Inspectors General Cite the Use of Professional Standards for Evaluation**

FISMA requires agency inspectors general to perform an independent evaluation of the information security programs and practices of their 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.

---

We have previously reported<sup>9</sup> that the annual inspector general independent evaluations lacked a common approach and that the scope and methodology of the evaluations varied across agencies. We stated that there was an opportunity to improve these evaluations by conducting them in accordance with audit standards or a common approach and framework. In their 2008 FISMA reports, more inspectors general indicated using professional standards (16) than had in their 2007 reports (8); in addition, 21 of 24 provided supplemental information about the agency's implementation of FISMA. The development and use of a common framework or adherence to auditing standards could provide improved effectiveness, increased efficiency, quality control, and consistency in inspector general assessments.

---

#### OMB Can Improve Annual Reporting and Oversight of Agencies' Information Security Programs

FISMA specifies that OMB is to develop policies, principles, standards, and guidelines on information security. Each year, OMB provides instructions to federal agencies and their inspectors general for FISMA annual reporting. Additionally, OMB summarizes the information provided by the agencies and the inspectors general in its report to Congress. We have previously made several recommendations to OMB for improving this annual reporting. OMB has required agencies to report systems information by risk category and reviewed its guidance to ensure clarity of instructions.

In addition to the previously reported shortcomings, OMB's reporting instructions for fiscal year 2008 did not sufficiently address several processes key to implementing an agencywide security program and were sometimes unclear. For example, the reporting instructions did not request inspectors general to provide information on the quality or effectiveness of agencies' processes for developing and maintaining inventories, providing specialized

---

<sup>9</sup>GAO, *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, GAO-07-837 (Washington, D.C.: July, 2007) and *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist*, GAO-08-571T (Washington, D.C.: March 12, 2008).

---

security training, and monitoring contractors. For these activities, inspectors general were requested to report only on the extent to which agencies had implemented the activity but not on the effectiveness of those activities. Providing information on the effectiveness of the processes used to implement the activities could further enhance the usefulness of the data for management and oversight purposes.

In addition, the guidance to inspectors general did not define or identify criteria for determining the level of performance in certification and accreditation for each rating. Not all inspectors general considered the same aspects in reviewing the certification and accreditation process, yet all were allowed to provide the same rating. Without clear guidelines for rating these processes, OMB and Congress may not have a consistent basis for comparing the progress of an agency over time or against other agencies.

In its report to Congress for fiscal year 2008, OMB did not fully summarize the findings from the inspectors general independent evaluations or identify significant deficiencies in agencies' information security practices. This information could be useful in determining whether agencies are effectively implementing information security policies, procedures, and practices.

OMB also did not explicitly approve or disapprove agencies' information security programs. FISMA requires OMB to review agencies' information security programs at least annually, and approve or disapprove them. As a result, a mechanism for establishing accountability and holding agencies accountable for implementing effective programs was not used.

In summary, as illustrated by recent incidents at federal agencies, significant weaknesses in information security policies and practices expose sensitive data to significant risk. Almost all major agencies reported weaknesses in one or more areas of information security controls during fiscal year 2008. Despite these persistent weaknesses, agencies reported increased compliance in implementing key information security activities. While the

---

inspectors general and OMB have made progress toward fulfilling their statutory requirements, OMB's annual reporting instructions did not cover key security activities and were not always clear. In addition, OMB did not include key information about findings and significant deficiencies identified by inspectors general in its governmentwide report to Congress and did not approve or disapprove agency information security programs. Shortcomings in reporting and oversight can result in insufficient or misleading information being provided to Congress and diminish its ability to monitor and assist federal agencies in improving the state of federal information security.

Chairwoman Watson, this concludes my statement. I would be happy to answer any questions you or other members of the subcommittee may have.

---

## Contact and Acknowledgments

If you have any questions regarding this report, please contact Gregory C. Wilshusen, Director, Information Security Issues, at (202) 512-6244 or [wilshuseng@gao.gov](mailto:wilshuseng@gao.gov). Other key contributors to this report include Charles Vrabel (Assistant Director), Larry Crosland, Neil Doherty, Nancy Glover, and Jayne Wilson.

Ms. WATSON. Thank you, Mr. Wilshusen.  
Ms. Patillo, you may proceed.

**STATEMENT OF JACQUELYN PATILLO**

Ms. PATILLO. Thank you. Good morning, Madam Chairwoman Watson and members of the subcommittee. Thank you for the opportunity to appear today to discuss the state of Federal information security and the Department of Transportation efforts to comply with the Federal Information Security Management Act of 2002.

I currently serve as the Department's Acting Chief Information Officer and Acting Senior Agency Official for Privacy.

The Department of Transportation Office of the Chief Information Officer has operational responsibility for the Departmental network and communications infrastructure, as well as providing shared services for the Office of the secretary and for an increasing share of employees in the DOT operating administrations as they transition toward use of DOT shared information services.

The DOT CIO's office also has overall responsibility for the Department's FISMA program and the cybersecurity posture of DOT networks and information systems. As part of those responsibilities, we must maintain situational awareness of the vulnerabilities and activities on DOT networks and systems, but also seek to mitigate identified vulnerabilities prior to exploitation in order to minimize risks to DOT, Federal, State, local and to the extent practicable, private systems and data.

Today's world of rapidly evolving threats, interconnected systems and telework vulnerabilities and risks have the potential to impact upon the other networks and interconnected systems. DOT is currently working to make improvements from its 2007 FISMA grade, and the DOT Inspector General's 2008 evaluation of the DOT cybersecurity program as "not effective." We developed an aggressive correction action plan to address the recommendations made by the Inspector General, instituted regular internal coordination with the DOT operating administrations to monitor and drive progress, as well as reallocating existing personnel and resources to focus on key areas for improvement such as certification and accreditation, verification and validation and awareness training.

As DOT continues to make improvements in cybersecurity and privacy, we know much remains to be done. Partnerships between the public and private sector to develop more intuitive and proactive mechanisms for dynamic prevention and detection of harmful behavior will facilitate a paradigm shift from a reactive mode to a more dynamic and proactive mode.

In conclusion, I would offer that the Department of Transportation has achieved considerable progress in securing its networks against intrusions and cyber-attacks. Nonetheless, there is no reason to celebrate nor time to rest. Again, thank you for the opportunity to comment on these important topics, and I look forward to answering any questions that you may have.

[The prepared statement of Ms. Patillo follows:]

**STATEMENT OF JACQUELYN PATILLO  
ACTING CHIEF INFORMATION OFFICER  
U.S. DEPARTMENT OF TRANSPORTATION**

**BEFORE THE  
SUBCOMMITTEE ON MANAGEMENT, ORGANIZATION, AND  
PROCUREMENT  
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM  
U.S. HOUSE OF REPRESENTATIVES**

**May 19, 2009**

Madam Chairwoman and members of the Subcommittee, thank you for the opportunity to appear today to discuss the state of federal information security, and the Department of Transportation's efforts to comply with the Federal Information Security Management Act of 2002 (FISMA).

I currently serve as the Department's Acting Chief Information Officer (CIO) and Acting Senior Agency Official for Privacy (SAOP).

The Department of Transportation (DOT) Office of the Chief Information Officer (OCIO) has operational responsibility for the Departmental network and communications infrastructure, as well as providing shared services for the Office of the Secretary and for an increasing share of employees in the DOT Operating Administrations as they transition towards use of DOT shared infrastructure services.

The DOT CIO's office also has overall responsibility for the Department's FISMA program and the cyber security posture of DOT networks and information systems. As

part of those responsibilities, we must maintain situational awareness of the vulnerabilities and activities on DOT networks and systems, but also seek to mitigate identified vulnerabilities prior to exploitation in order to minimize risks to DOT, Federal, state, local, and to the extent practicable, private systems and data. Where previously we might have limited our focus to just DOT systems and data, in today's world of rapidly evolving threats, interconnected systems, shared services, telework, and cloud computing, vulnerabilities and risks on a given network or system have the potential to impact upon the other networks and systems to which it may interface or be connected.

It is in that context that I come to you today to discuss DOT's FISMA program and progress towards compliance, peer-to-peer (P2P) software, and the recent report from the DOT Office of the Inspector General on FAA web application security.

#### **FISMA Status and Progress**

DOT is currently working to make improvements from its 2007 FISMA grade, and the DOT Inspector General's 2008 evaluation of the DOT cyber security program as "not effective." We developed a corrective action plan to address the recommendations made by the Inspector General, instituted regular internal coordination with the DOT Operating Administrations to monitor and drive progress, and reallocated existing personnel and resources to focus on key areas for improvement such as certification and accreditation, verification and validation, and awareness training.

We also have work underway to better define processes, procedures, and metrics for the DOT security program so as to ensure that processes are repeatable, measurable, and sustainable. In doing so, we are seeking to institutionalize these changes within DOT to improve both current and future FISMA performance and compliance, and enhance the resiliency of the program, while retaining sufficient flexibility for evolution of the program as requirements change. We are also actively participating in the White House cyber-security review and expect to implement guidance and recommendations from that effort as they are approved.

#### **Cyber Security Improvements and Institutionalizing Change**

On this front, in 2008 the DOT Secretary cemented the role of the DOT Cyber Security Management Center (CSMC) as the DOT enterprise Security Operations Center (SOC) agent for to the U.S. Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security, and established a governing Board of Directors to oversee operations and the strategic direction of the Cyber Security Management Center (CSMC). This action consolidated DOT's cyber security detection, protection, analysis, and response, and cyber security situational awareness in one entity, which streamlined incident handling and improved the detection of unauthorized activities on DOT networks.

Similarly, a pilot implementation of Network Admission Control (NAC) has become an integrated component of the remote access solution for teleworkers and staff working remotely who access the DOT Headquarters network. This Network Admission Control

(NAC) technology permits us to establish policy requirements for computers connecting to the network remotely. This allows DOT to check computers at the periphery before they are allowed access to the internal network. This mechanism checks – among other things – the presence of up to date virus protection, and the existence of peer-to-peer software on the computer requesting access to the DOT network. DOT policy prohibits the use of peer-to-peer software on any DOT asset or computing resources. Computers that fail to meet the requirements are either denied access completely, or are redirected to an isolated web site where patches and updated security software may be downloaded to become compliant.

This capability is also useful in addressing vulnerabilities with employee personal computers used for telework. While we do not scan personal computers used for telework at a detailed level, we can ensure that minimum security requirements are met. This capability was used during the Conficker incident earlier this year to ensure that computers connecting remotely through the DOT secure remote access (SRA) and virtual private network (VPN) systems had active local firewalls installed, and an active antivirus solution. We will be evaluating means to extend this capability to provide coverage at all points of entry into the DOT network.

Building upon Network Admission Control (NAC) and the Cyber Security Management Center (CSMC), we have continued our implementation of the Federal Desktop Core Configuration (FDCC), a configuration standard for Microsoft Windows computers published by the National Institute of Standards and Technology.

**Inspector General's Report on ATC Web Application Security**

On the subject of the DOT Office of the Inspector General's report on its "Review of Web Application Security and Intrusion Detection in Air Traffic Control Systems", we view the report and its recommendations as instructive not just for the Federal Aviation Administration, but for the other Operating Administrations in DOT and other federal agencies with complex information systems or critical infrastructure responsibilities. The reduction of vulnerabilities in our networks and systems, and mitigation of significant risks is a continuous process that evolves continuously as threat capabilities are ever changing. It requires constant vigilance and skilled individuals using the latest tools to reduce the risk of an attack, and to minimize any implications from an attack, should one occur, whether it comes from inside or outside of our networks.

We take our responsibility for cyber security seriously, and are appreciative of the renewed management attention that the Inspector General's report has drawn to areas where there are fresh opportunities for improvement.

We will be working with the FAA CIO to ensure that the corrective actions to address the issues identified in the report are appropriately implemented. Where there are opportunities to leverage activities, solutions, or lessons learned to the benefit of other DOT programs, we will work with the FAA CIO and the Operating Administration CIOs

to deploy solutions across the DOT enterprise in order to minimize risks to all connected systems and stakeholders.

### **Challenges Remain**

As DOT continues to make improvements in cyber security and privacy, we know much remains to be done. Partnerships between the public and private sector to develop more intuitive and proactive mechanisms for dynamic prevention and detection of harmful behavior will facilitate a paradigm shift from a reactive mode to a more dynamic and proactive one.

### **Summary**

In conclusion, I would offer that the Department of Transportation has achieved considerable progress in securing its networks against intrusions and cyber attacks. Nonetheless, there is no reason to celebrate, nor time to rest. Every day we are encountering new threats and new risks, and the capabilities for increasingly sophisticated attacks on critical information technology infrastructure continues to grow. The issues we face are larger than individual departmental CIOs and their staffs. Making progress towards greater network and computer security will be dependent upon effective leadership, both within agencies, and across the Federal government. Staying at least one step ahead of the next cyber attack will require vigilance rooted in a highly skilled IT workforce using the most capable and effective tools available from the private sector. Finally, our networks require the resilience and capabilities to ensure that any intrusions

that do occur are promptly detected, quickly and effectively dealt with, and the vulnerabilities that enabled the intrusion are swiftly remediated.

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

Ms. WATSON. Thank you, Ms. Patillo.  
Ms. Graves, you may proceed.

**STATEMENT OF MARGARET H. GRAVES**

Ms. GRAVES. Chairwoman Watson, Ranking Member Bilbray and members of the subcommittee, thank you and good morning. I am Margie Graves, the Acting CIO for DHS. Today I will discuss the state of information security at the Department of Homeland Security and our efforts to comply with the requirements established under the Federal Information Security Management Act of 2002.

In 2004, the Department of Homeland Security embarked on a multi-year strategy for bringing the Department into full FISMA compliance. In the ensuing 2 years, the Department conducted an enterprise-wide IT systems inventory and ensured that all systems completed a full risk assessment and a comprehensive certification and accreditation. Security requirements have also been built into the Department's Systems Engineering Life Cycle methodology and specific contract language in the Homeland Security acquisition regulations now expressly requires contractors to comply with applicable Department security policies.

In 2007, the Department's Enterprise IT Security Operations Center was chartered to provide a 24 by 7 computer incident handling capability for the Department. The original focus was to mitigate the effects of standard viruses, worms and other forms of malicious payloads that do not directly target any specific agency or group. But by late 2007, it had also become apparent that in addition to these non-specific threats, there was a growing class of sophisticated actors who directly targeted the Department, especially our leadership.

To address these threats, the Department created its own internal focused operations team to better understand enterprise risk associated with targeted attacks and to develop and deploy responses capabilities to deter them. In addition to our full commitment to implementing all Federal IT security initiatives, DHS is now pursuing several enterprise consolidation and enhancement efforts as part of an overall defense-in-depth strategy to better confront these threats.

All of these initiatives are supported in the President's fiscal year 2010 budget that was recently submitted to Congress for approval. Specific initiatives include the following: first, the Department is committed to fully implementing all requirements of the Homeland Security Presidential Directive 12, including logical access for IP systems. Second, the one OneNet project is a major Department initiative for collapsing legacy wide-area networks into one enterprise network. The Department is transitioning all components into mission-unique Trust Zones through the implementation of a series of Policy Enforcement Points beginning in 2010. Third, we are adding features to the Trusted Internet Connections that will allow us to further improve our ability to detect and respond to malicious emails.

Finally, the Department's data center consolidation project provides the plan for migrating DHS systems to two enterprise data centers that are currently protected by our Trusted Internet Connections and that have been designed to address sophisticated

threats. These two data centers now deliver utility computing and infrastructure as a Service, allowing DHS to realize benefits of cloud computing while also providing the security so necessary for the threats we face today.

I would also like to acknowledge the great work that the U.S. Computer Emergency Readiness Team [US-CERT], is doing on behalf of Federal agencies. US-CERT is deploying Government-specific centers called Einstein that are designed to provide alerts regarding sophisticated actors who directly target the Federal Government. Einstein centers are now deployed at both the Department's Trusted Internet Connections and they are providing critical alerts to the focused operations team.

As a result of the original FISMA statute, Federal agencies now have a good road map for designing and implementing agency-wide information security programs. The statute provides a strong foundation on which to build. However, we have seen over the last few years that sophisticated threat actors are becoming more persistent and more aggressive. Therefore, each and every agency must also develop in-house focused operations capability to improve overall situational awareness about these sophisticated actors and to be ready to respond effectively whenever there is any indication of a targeted attack.

The Department welcomes the opportunity to work with Congress in developing any future strategy that will not only build on past successes, but that will also remain relevant and effective in today's evolving IT security threat environment.

Thank you.

[The prepared statement of Ms. Graves follows:]

**TESTIMONY OF  
Margaret H. Graves  
Acting Chief Information Officer  
U.S. Department of Homeland Security  
Before the  
House Oversight and Government Reform  
Subcommittee on Management, Organization, and Procurement**

**May 19, 2009**

Chairwoman Watson, Ranking Member Bilbray, and Members of the committee, thank you and good morning. Today, I will discuss the current state of information security at the Department of Homeland Security (DHS) and our efforts to comply with the requirements established under the Federal Information Security Management Act of 2002 (P.L. 107-347).

The Federal Information Management Act of 2002 (FISMA) was originally enacted in the same year that the Department of Homeland Security was created. In a sense, both the Department and the statute have grown up together, and, for this reason, it is certainly appropriate for the Department to comment on the state of implementing FISMA requirements in the federal government. Thank you for that opportunity.

As the Acting Chief Information Officer (CIO) for DHS, I am regularly confronted with a wide range of issues associated with delivering robust and effective information technology (IT) services for one of the largest agencies in the Federal government. The requirements for IT services in the Department are just as diverse as are our missions; from protecting our borders, to securing air travel, to protecting key government officials, to providing immigration services, to managing Federal response after a disaster, and many other missions that are equally important.

The Department's complex IT infrastructure must support all of these diverse missions, each with their own unique IT requirements. To do this, DHS is leveraging the power of information technology to bring them together under a common, shared enterprise communications backbone. None of this would be possible without a strong information security program that not only fully implements the original Federal information security vision of Congress back in 2002, but also meets both the letter and the spirit of the FISMA statute as currently enacted.

In 2004, the Department of Homeland Security embarked on a multi-year strategy for bringing the Department into full FISMA compliance. In 2005, the Department conducted a comprehensive, Department-wide IT systems inventory. Today there are approximately 600 major systems in use in the Department. Approximately one-third of these systems reside in contractor facilities; however, all systems regardless of whether they reside in government or contractor facilities are required to undergo a full certification and accreditation prior to becoming operational. In 2006, all systems – both government and contractor operated - completed a full certification and accreditation to ensure that appropriate system-specific controls were in place. I should also point out that every system in the FISMA inventory is required to complete a risk assessment as part of the certification and accreditation process, and every risk assessment is reviewed by the Office of the CIO

We have also made great strides in improving our IT business processes, especially in the area of security compliance. The Department's Systems Engineering Life Cycle program requires security review at all appropriate key decision points. The Homeland Security Acquisition

Regulation includes specific contract language that expressly requires contractors to comply with applicable Department security policies. Additionally, the Office of the CIO reviews and approves all IT acquisitions over \$2.5 million in the aggregate, and Component CIOs are required to review and approve IT acquisitions for any level of funding. This includes specific vetting to ensure that applicable security requirements are fully incorporated into each IT contract.

In 2007, the Department's Enterprise IT Security Operations Center (DHS SOC) was chartered to provide a 24X7 computer incident monitoring, handling, and response capability for the Department, and today this Center is the central coordinating and reporting authority for all computer security incidents throughout the Department. The primary focus of the DHS SOC has always been to mitigate the effects of the pervasive "Internet pollution" that permeates the Internet today. These threats include standard viruses, worms, and other forms of malicious payloads that do not directly target any specific agency or group. Mitigation activities for these threats include deploying commercially-provided antivirus protection; entry and egress proxy services and filtering, to include email filtering for SPAM; oversight and management for installing vendor provided software patches; aggressive scanning for evidence of infections; and a comprehensive Department-wide incident reporting and handling program.

By late 2007, it had also become apparent that in addition to these non-specific threats, there was a growing class of sophisticated actors who directly targeted the Department. For this reason, the Department created its own internal Focused Operations Team to improve situational awareness about these sophisticated actors, to better understand enterprise risk associated with

targeted attacks, and to develop and deploy response capabilities to deter them. This team is chartered under the DHS CIO and includes key representatives from the Office of Security, the Office of Intelligence and Analysis, and the DHS Security Operations Center. Appropriate CIOs and system owners from our components are also represented on a case-by-case basis. All DHS SOC personnel have been trained to look for and recognize incidents of special concern and that require more detailed analysis by the Focused Operations Team.

We have now learned first-hand about this growing category of threats that directly target the Federal government, our systems, and our information. We have also witnessed how these threats have become more persistent, more pervasive, and even more aggressive than we imagined. These actors appear to be highly-motivated and well-resourced, and it will take all of our collective efforts to keep them out of our networks. For this reason, the Department is fully committed to implementing all Federal IT security initiatives; including, deploying Trusted Internet Connections; complying with the Federal Desktop Core Configuration initiative; fully implementing Homeland Security Presidential Directive 12, to include logical access; and hardening our Domain Name Servers (DNS) with the use of the DNS Security protocol.

Over the last two years, the Department's Focused Operations Team has also provided some key recommendations for other internal enterprise security enhancements as part of an overall defense-in-depth strategy, and all of these initiatives have been specifically developed to better confront these sophisticated actors. Three enterprise consolidation initiatives are at the core of these efforts. All of these initiatives are fully supported in the President's fiscal year 2010 budget

that was recently submitted to Congress for approval, and I would ask for your support for them.

Specific initiatives include:

1. "OneNet" is a major Department initiative for collapsing legacy wide-area networks (WAN) into one enterprise WAN. Each major component necessarily requires a unique set of IT security policies in support of their diverse missions, and these policies must be resolved separately in order to facilitate information sharing across a single, shared, enterprise wide-area network. Without the ability to effectively resolve these policy differences at the enterprise-level, either (1) information sharing will be severely limited, or, (2) the enterprise will naturally devolve to the least common denominator at the expense of protecting sensitive mission data.

For these reasons, the Department is transitioning all Components into mission-unique Trust Zones through the implementation of a series of Policy Enforcement Points (PEPs) beginning in 2010. PEPs are comprised of hardware and software packages positioned throughout the network, as well as appropriate management functions at the SOC. Specifically, each PEP will include an enterprise-managed firewall to resolve policy differences, and sophisticated monitoring capabilities that will provide the SOC with enhanced visibility across the entire enterprise. This enhancement will provide the ability to track and respond to sophisticated threat actors that now regularly target the Department.

2. Currently, phishing emails are the number one attack vector for adversaries who directly target DHS and our leadership. There are usually over 100 of these a week, and while we have

improved our ability to detect malicious emails at the perimeter, we must continue to engage at multiple levels in the phishing email battle. Security controls for email must be strengthened, and we are adding some email specific features to the Trusted Internet Connections that will allow us to further improve our ability to detect and respond to malicious emails.

3. The Department's Data Center Consolidation Program has now delivered two world-class enterprise data centers, each with a number of enhanced security controls to ensure high-confidentiality, high-integrity and high-availability for applications residing in the data centers. Additionally, each data center now houses one of the two Trusted Internet Connections that have been designed with sophisticated threats in mind. Further, the Department's new data centers deliver utility computing and Infrastructure as a Service, allowing DHS to realize the benefits of cloud computing while also providing the security so necessary for the threats we face today. We are in the process of migrating applications to the data centers and in this way we will improve protection and monitoring for those applications.

At this time I would like to acknowledge the great work that the United States Computer Emergency Readiness Team (USCERT) is doing on behalf of Federal agencies. A few years ago, US-CERT began deploying a new set of government-specific sensors that are specifically designed to alert on these sophisticated threats. This monitoring capability is called "Einstein" and of the 55 Einstein 1 sensors that were originally deployed government-wide, 17 have been deployed specifically to protect the DHS network perimeter. More recently, an enhanced version of Einstein has also been developed by US-CERT, and the first Einstein 2 sensor was deployed at the Department's Trusted Internet Connection at the DHS data center in Mississippi. A second

Einstein 2 sensor is also now deployed at our other Trusted Internet Connection at our second data center in southern Virginia. These sensors are a key component of our overall monitoring program and have greatly improved our ability to detect attacks in near real time, so that we can implement appropriate mitigation efforts before major damage occurs. The Department conducted a Privacy Impact Assessments for (PIA) the original Einstein system and the updated Einstein 2 system. These two PIAs are available on [www.dhs.gov/privacy](http://www.dhs.gov/privacy) and serve both to explain how the system works and additional privacy protections DHS builds into its approach to information security.

As you can see, DHS has significant experience operating within the FISMA framework and it is clear to me that the original FISMA statute advanced the state of cybersecurity. It correctly places IT security accountability with three key individuals, the Agency Head, the Chief Information Officer, and a Senior Agency Official for Information Security, commonly referred in most federal agencies as the Chief Information Security Officer or CISO. The statute directed the National Institute of Standards and Technology (NIST) to develop both standards and guidance, and today the NIST IT security framework is considered to be the gold standard for security controls implementation. The statute also mandates annual, independent information security program reviews by the Inspector General, to ensure transparency and accountability. Finally, the statute acknowledges the fact that the real mission of the federal government is to provide a wide-range of diverse services to our citizens, by taking a risk-based approach to information security. Because of FISMA and the hard work of Federal employees to implement it, the federal government has made significant progress in strengthening our IT security posture.

Also as a direct result of the original FISMA statute, Federal agencies now have a comprehensive framework for implementing system-level controls, and these controls provide a strong foundation on which to build. Specifically within DHS, we have institutionalized all statutory requirements into our programmatic so that all system owners are building in security requirements as a matter of course. In addition, the DHS CISO ensures that security requirements are met at every stage of the system life cycle.

What is also apparent is that simply maintaining a controls framework alone is not enough. Sophisticated threat actors are persistent and aggressive, and despite our best efforts at maintaining effective controls, it is highly likely that these actors will from time-to-time be at least initially successful. We must count on this, plan for this, and be ready to act, so that a small problem doesn't become a big one. This means that in addition to implementing and maintaining strong system-level controls, and fully deploying government programs that are available, like those provided by USCERT, each and every agency must also develop in-house capabilities to improve overall situational awareness, especially with respect to enterprise network and systems transparency, and to be ready to respond quickly and effectively whenever there is any indication that an attack has begun. This means that CIOs and CISOs must have dedicated teams in place to monitor for, assess, and respond to these sophisticated actors. Team members must be cleared to appropriate levels to ensure they have the necessary situational awareness for dealing with these actors. Organizational processes must also be instituted so that the team can quickly engage with system owners, program managers, and agency leadership to ensure effective and timely responses that are consistent with overall mission objectives for the agency.

DHS has made significant and measurable progress in implementing all of the FISMA requirements, and, the enterprise security initiatives I have outlined represent major steps for improving the Department's overall security posture. But there is always more that can be done by both the Administration and the Congress in the area of Federal IT security management. The Department welcomes the opportunity to work with Congress in developing any future strategy that will not only build on past implementation successes, but also remain relevant and effective in today's ever changing IT security threat environment.

Ms. WATSON. Thank you, Ms. Graves.  
Mr. Chun, you may proceed.

#### STATEMENT OF SAMUEL CHUN

Mr. CHUN. Good morning, Chairwoman Watson and distinguished members of the subcommittee.

On behalf of EDS, an HP company, thank you for the opportunity to discuss our perspectives on this important topic of Federal information security. For nearly 45 years, EDS has been a trusted ally, serving governments across the world. As one of the largest providers of technology services and solutions to the U.S. Government, we strive daily to achieve secure operational excellence in everything we do.

From the millions of warfighters that carry our identity credentials to the one in five citizens who used our voter registration and election management systems last fall, we are entrusted with some of the most sensitive information of our fellow citizens. We understand and appreciate the enormous cybersecurity challenges that our Government agencies face today.

We can attest definitively to the fact that the well-publicized threats facing our information infrastructures are real. Since our founding, we have built and managed on behalf of our Government customers, some of the largest and most complex systems and networks in existence. This includes the Navy Marine Corps Intranet, which is the largest purpose-built network in the world. We currently manage 180 data centers, 380,000 servers, 5.4 million desktops and nearly 15 million Internet IP addresses. And we, like everyone else, are constantly under attack.

We are also finding the number, type and sophistication of the attacks to be growing. We expect these trends to continue.

FISMA was enacted nearly 7 years ago to require Federal agencies to improve the security postures of their information systems by implementing a program that would reduce security risks. While the debate rages as to whether FISMA is an effective engine for measuring and improving security performance, there is little doubt as to its good intentions.

While there are numerous positive benefits provided by FISMA, there is general consensus that FISMA does in fact need reform. We have observed and participated in many passionate debates about FISMA and have concluded the following deficiencies need to be addressed. First, compliance has become too administrative, emphasizing paperwork. Second, the correlation between compliance and operating performance is unclear. Three, accountability for good and poor compliance is also unclear. Fourth, the validity of what is being measured under FISMA is in question. And five, rapidly emerging threats may be outpacing compliance efforts.

Our vision for information security for our customers is simple. Security should be so tightly integrated into the core of agency operations that stakeholders have the confidence to be agile at the edge. To put it simply, security should be an embedded part of operations that permeates across the enterprise.

By no means to do we think this will be an easy or short journey. In fact, we expect the vision will include some difficult decisions and foundational changes that will require champions, resources,

technologies and definitely the wisdom of time. That said, I think we would be remiss were we not to discuss the first steps and big challenges that must be addressed to take the first positive steps toward our vision.

First, governance. Because of threats against our information systems and our infrastructures can appear without warning, and the defense cycles required could be in seconds, lawful orders that change an agency's infrastructure must be carried out quickly and comprehensively across the Government enterprise. This highlights the need for clear and consistent roles, responsibilities, policies and accountability structures for the Government enterprise.

Second, consolidation. Consolidating and standardizing infrastructures facilitates situational awareness, nearly impossible when an agency depends on myriad small, independently operating networks and enclaves.

Three, consistent protection. Because Government infrastructures are vast and interconnected, applying consistent, enterprise-wide defense in-depth strategies strongly improves security performance.

Four, emphasis on operating performance. We support the efforts to clearly articulate and require operating thresholds for security of acquisitions to better meet them.

Then finally, people. Security practitioners clearly must be trained, vetted and industry-certified on the best security policies, technologies and practices. We need to continue the trend of raising a much larger cybersecurity work force.

In summary, we believe security must be tightly integrated with operations in agencies. It will take a conscious effort by operators and users, Government and industry alike, for the inventing of security into everything we do. For nearly 50 years, EDS has been an ally for governments in tackling some of the most difficult challenges that face them. We continue to stand by, ready to work with you on this one.

Thank you, and I will be happy to answer your questions.  
[The prepared statement of Mr. Chun follows:]

49

**TESTIMONY BY**

**SAMUEL CHUN**

**DIRECTOR, CYBER SECURITY PRACTICE**

**EDS U.S. PUBLIC SECTOR,**

**A HEWLETT – PACKARD COMPANY**

**BEFORE THE U.S. HOUSE OF REPRESENTATIVES**

**SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,  
ORGANIZATION, AND PROCUREMENT**

**ON**

**“THE STATE OF FEDERAL INFORMATION SECURITY”**

**TUESDAY, MAY 19, 2009**

Good morning Chairwoman Watson, Ranking Member Bilbray, and members of the Subcommittee on Government Management, Organization, and Procurement.

On behalf of EDS, an HP Company, thank you for the opportunity to discuss our perspectives on this important topic of federal information security. For nearly 45 years EDS has been a trusted ally, serving governments across the world. As one of the largest providers of technology services and solutions to US federal and state and local governments, we strive daily to achieve secure operational excellence in everything we do.

From the millions of war fighters who carry our identity credentials to the one in five citizens who used our voter registration and election management system last fall , we are entrusted with some of the most sensitive information of our fellow citizens. We understand and appreciate the enormous cyber security challenges that our government agencies face today.

We can attest definitively to the fact that the well-publicized threats facing our information infrastructures are real. Since our founding we have built and managed, on behalf of our government customers, some of the largest and most complex systems and networks in existence. This includes the Navy Marine Corps Intranet (NMCI), the largest purpose-built network in the world. We currently manage 180 data centers, 380,000 servers, 5.4 million desktops and nearly 15 million IP addresses. And we, like everyone else, are constantly under attack. We are also finding the number, type, and sophistication of the attacks to be growing. We expect these trends to continue.

The Federal Information Security Management Act of 2002 was enacted to require federal agencies to improve the security postures of their information systems by implementing a program that would reduce security risks. There is little doubt as to the good intent of FISMA. However, as members of TechAmerica and the Business Software Alliance, we have first-hand knowledge of the debate that rages as to whether FISMA is an effective engine for measuring and improving security performance at agencies. A dispassionate review of FISMA over the last seven years since its enactment yields some tangible benefits that should be acknowledged before we review how FISMA should be reformed to be more effective.

First, it clearly identified (Sec. 3541) that both information security and the role that the private sector plays in it are vital to the national and economic security of the United States. Second, FISMA identified key agencies, specifically NIST and OMB, to set the standards for and oversee security management. By doing so, it provided a government-wide approach that clearly identified processes for inventorying, testing, certifying, accrediting and auditing of systems. This, in turn, provides us, the government integrator community, with a uniform of set of standards and guidelines to follow when implementing systems on behalf of agencies. NIST and its 800 series of special publications are of especially worthy of note as they are relied upon by nearly everyone in the integration community.

While the positive contributions of FISMA are apparent, there is general consensus that FISMA does, in fact, need reform. We've observed and participated in many passionate debates about the effectiveness of FISMA and have concluded that the following deficiencies need to be addressed:

1. Compliance has become too administrative. This is the single most common feedback we hear about FISMA. There is too much emphasis on the generation of paper reports for compliance, certification and accreditation, and auditing. Some have even suggested that it detracts both time and resources away from the real attention required to secure systems. Whether it's by automation or a change in the way reporting is done, action must be taken to reduce the administrative burden of compliance from the agencies.
2. The correlation between compliance and operating performance is unclear. We've observed that some of the most well defended agencies consistently receive poor report cards. In addition, a single grade assigned to a large and diverse agency with many components only generalizes the picture and may not, in fact, provide proper warning of a material vulnerability to mission performance to the agency's mission owners. A more granular approach to reporting that highlights operating performance -- in addition to compliance -- will likely provide more clarity.

3. Accountability for good and poor compliance is unclear. Many have asked what purpose report cards serve other than to paint a broad, general picture of performance for general consumption. While enormous effort is expended in providing these reports and answering audits, it is not transparent how that information is used for the purposes of budgeting, rewards, and assigning accountability. For system integrators, however, there is a clear process for receiving and maintaining the authority to operate through the certification and accreditation process that impact us directly. There should be equally transparent accountability for poor performance. We reiterate our support for the appointment of a new cyber official who can address these concerns.
4. Validity of what is being measured under FISMA is in question. Compliance to FISMA measures how well an agency has accounted for, and applied risk and security management standards, processes, and plans for, information systems. The inference is that as long as the standards, processes and plans are sound, the operational security of an agency is thereby effective. We've observed that much of the debate about FISMA revolves around whether such indirect measures of security required by FISMA compliance adequately ensure operational security performance.

Direct measures of security performance, such as tracking the number of attacks defended against; the mean time to patch a vulnerability; the number of incidents to which an agency has responded; or the percent of applications tested would provide more rigorous and intensive measures of security. While they provide a much higher level of confidence in the operating performance of a system, they are limited by the sheer scale, size, and scope of the systems being managed in federal agencies. Such real time measures and reporting of agency security performance could enhance both actual security as well as the oversight function. We suggest real rigor and analysis on what combination of measurements will result in the best operating picture of agency so that real insight on the operating picture of an agency is reported.

5. Rapidly emerging threats may be outpacing compliance efforts. Although NIST has been instrumental in setting the standards and processes necessary for industry and

government to conform to, it is unlikely that these standards will keep pace with the rapidly emerging threats. Other organizations such as the US-CERT and the NSA have far greater insight into the emerging threats facing federal agencies. While compliance to standards and processes is essential, we must integrate expertise from other organizations that provide a more real time view into the threats out there in order to be better prepared to meet them in our operations.

Our vision for information security for our customers is simple. Security should be so tightly integrated from the core that agencies have the confidence to be agile at the edge. To put it simply, security should be an embedded part of operations that permeates across the enterprise. Stakeholders should be able to confidently share, receive, and use information with friends and allies without being distracted by concerns of security. By no means, do we think this will be an easy or short journey. In fact we expect this vision will include difficult decisions and foundational changes that will require champions, resources, technologies and definitely the wisdom of time.

That said I think we would be remiss were we not to discuss the first steps and big challenges that must be addressed to take the first positive steps toward our vision.

1. **GOVERNANCE:** A strong central governance of information infrastructure is vital in defending against cyber threats. Because the threats against information systems and networks can appear without warning, and defense cycle times can be just seconds, lawful orders that change an agency's infrastructure must be carried out quickly and comprehensively throughout the government enterprise. It is not inconceivable that an attack against our government infrastructures could require that rapid changes be made across the entire government enterprise. This highlights the need for clear and consistent roles, responsibilities, policies and accountability structures for the government. Consequently, we strongly support the creation of a new and empowered leader to spearhead this effort.

2. **CONSOLIDATION:** Consolidating and standardizing infrastructure improves situational awareness, nearly impossible when an agency depends on myriad small, independently operating networks and monitoring systems. Instead, consolidating such networks into fewer, larger tightly controlled operations, such as NMCI, substantially improves security awareness and control. A standardized approach to IT, like the Federal Desktop Core Configuration, substantially improves security by enhancing configuration and change management capabilities as well as baseline security levels. We see substantial benefits in reducing the sheer number and type of networks and infrastructures that operate in agencies.
3. **CONSISTENT PROTECTION:** Because government infrastructures are vast and interconnected, applying consistent, enterprise wide defense in-depth strategies strongly improves security performance. Recognizing that no single countermeasure is effective against every threat layering of defenses consistently – which includes technologies, processes, and people – mitigates much of the risk. While building layers of defenses to protect systems, networks and the data they carry can be expensive and sometimes impacts user satisfaction, it is a vital strategy in protecting cyberspace. While the urge might be to think of new technologies and tools, we see real need in consistency and enterprise approach as a vulnerability in one area may have potential unintended legacies for everyone.
4. **EMPHASIS ON OPERATING PERFORMANCE:** While we comply with the various regulatory and audit requirements of our customers, we continue to focus on achieving secure operational excellence by continually reviewing our operating metrics relative to our customer's needs to fulfill their missions. We have recently observed that there has been increased effort during the acquisition process to clearly identify operating performance for security. In particular we've observed enhanced requirements for vulnerability management, incident response, and compliance to standards. We support these efforts to clearly articulate the operating thresholds for security to better meet them.

5. PEOPLE: Lastly we have to focus on our people. Security practitioners clearly must be trained, vetted and industry certified on the best security policies, technologies and practices. This is an area where we have seen substantial progress in industry and government as information security has become a clear and distinct discipline within technology. We need to continue the trend of raising a much larger cyber security workforce.

In summary, we believe secure operational excellence is what we're trying to achieve by reforming FISMA. Security must be more tightly integrated with operations and it will take a conscious effort by operators and users, government and industry alike for embedding security into everything we do -- including technology. For nearly 50 years, EDS has been an ally for governments in tackling some of the most challenging issues that face them. We continue to stand ready to work with you on this one.

Thank you. I'll be happy to answer any questions you might have.

Ms. WATSON. Thank you, Mr. Chun.  
Mr. Shoer, please proceed.

**STATEMENT OF M.J. SHOER**

Mr. SHOER. Good morning, Chairwoman Watson, Ranking Member Bilbray, Congressman Connolly and Congressman Duncan.

Chairwoman Watson, I want to thank you for your acknowledgement of my daughter. I appreciate that. I wanted her to have the opportunity to see our participatory Government working quite well.

Ranking Member Bilbray, I think you will find that my testimony will address some of the concerns that you articulated quite directly.

On behalf of the Computing Technology Industry Association [CompTIA], we thank you for your ongoing interest in the state of Federal information security. This is a broad, yet critical subject, ranging from FISMA as well as a variety of practices that impact our national security, citizenry and the computing industry at large. We appreciate the opportunity to share with you the following views.

CompTIA is the voice of the world's \$3 trillion information technology industry. CompTIA's members include thousands of small businesses called value-added resellers [VARs], as well as nearly ever major computer hardware manufacturer, software publisher and services provider. Based upon a recent CompTIA survey, we estimate that 1 in 12, or about 12 million American adults, consider themselves to be an IT worker. This is larger than the number of American adults classified by the BLS as employed in farming, mining and construction combined. This is also close to the number of adults classified by BLS as working in manufacturing or transportation. CompTIA has concluded that the IT work force is now one of the largest and most important parts of the American political community.

My name is M.J. Shoer, I am the president and virtual chief technology officer of a VAR, the Jenaly Technology Group, and I am pleased to be testifying on behalf of CompTIA. I live in Portsmouth, NH, and have been an information technology entrepreneur. In 1997, I founded Jenaly and have since served as its president.

On behalf of CompTIA and its many small business member companies, we welcome the subcommittee's exploration of FISMA and its effectiveness for today's ever-increasing cybersecurity challenges. Certainly, many critics and the other witnesses, including the GAO, have commented on the effectiveness of FISMA.

Recently, the GAO submitted 12 recommendations to the House of Representatives. One finding in particular, the eleventh, is significant for your attention. The finding calls for increasing the cadre of cybersecurity professionals, and the report states the following, "Expert panel members that actions should include making the cybersecurity discipline a profession through testing and licensing."

In summary of my written testimony, the issue before us all is how to enhance the security of critical Federal systems and protect our country and its citizenry. It is evident to critics or anyone who

regularly reads the newspaper that the current awareness training model is not working. Security breaches among the agencies have increased instead of falling off. This may be due to a disturbing phenomenon, namely, the lack of adequate personnel training and testing.

In contrast, I fear that all too often, the answer is a tendency to invest in technological solutions alone. Certainly, firewalls and encryption are part of the solution. However, the real cybersecurity equation lies in managing the balance between technology and human capital through training, testing and certification.

It is unfortunate we have so many challenges today, because the Congress came very close to requiring certification of Federal IT security workers in 2002. FISMA itself only requires security awareness training to inform impacted personnel of information security risks associated with their activities and to comply with agency procedures. The undisputed evidence concerning breaches reveals that this is insufficient for the Federal Government's needs.

In my view, I agree with the critical about several key flaws with the current FISMA framework. First, the fundamental flaw of the FISMA framework and the Federal Government's policy is a lack of emphasis on the training and testing that is vital. My recent meetings with various Hill staff confirms this, after my hearing episode after episode about breaches in the Federal system caused by human error, for example, the removal of a laptop from a Federal site and then improperly securing it while outside that site.

A second and significant flaw is the lack of uniform verifiable IT security training as the single largest problem regarding information security and the Federal Government. Fortunately, a solution to FISMA's flaws may be found elsewhere in the Federal system. In 2004, the Department of Defense has raised the bar for cybersecurity through a training and testing program commonly known as the 8570 Directive. This initiative focuses on the certification of personnel. Based upon my own experience in this industry, I believe that accreditations and certifications offer many benefits, including lower transaction costs. Remarkably, throughout the Federal Government only the DOD has formally required its employees and contractors to get certified.

Last year, my own IT business, Jenaly Technology Group, became the first in the country to become accredited for best practices in information security as it relates to our clients.

In conclusion, it is undisputed that we must protect the American public by having a security framework that guards information systems for both our Federal critical systems as well as the private sector. The computing industry is hard at work facing the unprecedented challenges of securing our data from both malicious threats and human error. Congress' enactment of the FISMA has provided a base level of protection.

The key to securing our Federal IT systems for the future lies in the partnership between technology and human capital. By effectively managing both technology and the people in concert through training and testing, such as through the certification process, we can win the battles in the security war. The current Defense Department model surrounding the 8570 Directive is a model worthy for emulation throughout the Federal Government. Any modifica-

tion of FISMA must recognize the lessons surrounding the human capital contribution to the IT security equation by the certification and accreditations to enhance our security.

Thank you very much, and I look forward to answering any questions.

[The prepared statement of Mr. Shoer follows:]

M. M. J. Strick



**The Computing Technology Industry Association**

**"The State of Federal Information Security"**

**Committee on Oversight and Government Reform**

**Subcommittee on Government Management, Organization, and Procurement**

**U.S. House of Representatives**

**Tuesday, May 19, 2009**

Dear Chairwoman Watson, Ranking Member Bilbray, and Members of the Committee:

On behalf of the Computing Technology Industry Association (CompTIA), we thank you for your ongoing interest in the "State of Federal Information Security." This is a broad, yet critical subject ranging from the "Federal Information Security Management Act of 2002" ("FISMA") (P.L. No. 107-347), as well as a variety of practices that impact our national security, citizenry, and the computing industry at large. We appreciate the opportunity to share the following views.

The Computing Technology Industry Association (CompTIA) is the voice of the world's \$3 trillion information technology industry. CompTIA membership extends into more than 100 countries and includes companies at the forefront of innovation; including, the channel partners and solution providers they rely on to bring their products to market, and the professionals responsible for maximizing the benefits organizations receive from their technology investments. The promotion of policies that enhance growth and competition within the computing world is central to CompTIA's core functions. Further, CompTIA's mission is to facilitate the development of vendor-neutral standards in e-commerce, customer service, workforce development, and ICT (Information and Communications Technology) workforce certification.

CompTIA's members include thousands of small computer services businesses called Value Added Resellers ("VARs"), as well as nearly every major computer hardware manufacturer, software publisher and services provider. Our membership also includes thousands of individuals who are members of our "IT Pro" and our "TechVoice" groups. Further, we are proud to represent a wide array of entities including those that are highly innovative and entrepreneurial, develop software and hold patents. Likewise, we are proud to represent the American IT worker whom relies on this technology to enhance the lives and productivity of our nation. Based upon a recent CompTIA survey, we estimate that

CompTIA  
FISMA Testimony  
May 2009

one in twelve, or about 12 million American adults, consider themselves to be IT workers.<sup>1</sup> This is larger than the number of American adults classified by the Bureau of Labor Statistics (“BLS”) as employed in farming, mining, and construction combined. This is also close to the number of adults classified by BLS as working in manufacturing or transportation. CompTIA has concluded that the IT workforce is now one of the largest and most important parts of the American political community.

My name is M.J. Shoer, the President and Virtual Chief Technology Officer of a VAR, the Jenaly Technology Group and am testifying on behalf of CompTIA. I live in Portsmouth, New Hampshire, and have been an information technology entrepreneur. In 1997, I founded Jenaly Technology Group and have since served as its President. Jenaly Technology Group provides IT services to small businesses throughout the region. In my current role, I am active in several IT groups and regularly write about information technology and small business issues.

#### **FISMA and the Current Federal Security Ecosystem**

On behalf of CompTIA and its many small business member companies, we welcome the Subcommittee’s exploration of FISMA and its effectiveness for today’s ever increasingly cybersecurity challenges. Certainly many critics and the other witnesses, including the Government Accountability Office (GAO), have commented on the effectiveness of FISMA. Recently, the GAO submitted twelve recommendations to the House of Representatives.<sup>2</sup> One finding, in particular, the eleventh, is significant for your attention. This finding calls for “increasing the cadre of cybersecurity professionals,” and the report states the following:

**Increasing the cadre of cybersecurity professionals** – The strategy includes efforts to increase the number and skills of cybersecurity professionals but, according to panelists, the results have not created sufficient numbers of professionals, including information security specialists and cybercrime investigators. Expert panel members stated that actions should include . . . making the cybersecurity discipline a profession through testing and licensing.<sup>3</sup>

It is unfortunate we have so many challenges today because the Congress came very close to requiring certification of federal IT security workers in 2002. FISMA itself only requires “security awareness training” to inform impacted personnel of information security risks associated with their activities, and to comply with agency procedures. The undisputed evidence reveals that this is insufficient for the federal government’s needs.

It is evident to critics, or anyone who regularly reads the newspaper, that the current awareness training model is not working. Security breaches among the agencies have increased instead of falling

<sup>1</sup> <http://www.comptia.org/issues/us.aspx>.

<sup>2</sup> *National Cybersecurity Strategy, Key Improvements Are Needed to Strengthen the Nation’s Posture*, GAO Rep. No. 09-432 (Mar. 10, 2009).

<sup>3</sup> *Id.* at 12. (emphasis added).

CompTIA  
FISMA Testimony  
May 2009

off. This may be due to a disturbing phenomenon. Recent GAO analysis compiling agency FISMA reports, the total employees and contractors receiving security awareness training fell from 91 percent in FY 2006 to 84 percent in FY 2007. Nine agencies reported a decrease in awareness training. One Inspector General reported that the agency was unable to ensure contractors received awareness training. Eight Inspectors General disagreed with their agency's estimation of individuals receiving security awareness training.

#### **A. FISMA: Identification of Fundamental Flaws**

In my view, the fundamental flaw of the FISMA framework and the federal government's policy is a lack of emphasis on the training and testing that is vital. My recent meetings with various Hill staff confirms this, after my hearing episode after episode about breaches in the federal system caused by human error (*e.g.*, removing a laptop from a federal site and improperly securing it).

A second and significant flaw is the lack of uniform, verifiable IT security training as the single largest problem regarding information security in the federal government. According to CompTIA's 7<sup>th</sup> ANNUAL TRENDS IN INFORMATION SECURITY SURVEY,<sup>4</sup> 59 percent of government respondents attributed their security breaches to human error. In addition, 25 percent of federal government employees reported not having a written security policy. From 2007-2008, the percentage of government agencies that required security training for IT staff fell from 70 percent to 60 percent.

Today, I would like to share some of my observations, as someone who has dedicated his career to information technology and security, regarding ways of enhancing FISMA for the challenges we face today and beyond. The basic themes of my recommendations are that the human element to data security requires greater attention; security awareness training is not a sufficient solution; and, the Pentagon's 8570 approach to IT security training should be adopted by the federal government to provide training and certification needs to keep federal IT cyber secure. Further, many critics believe that the threat posed by "human error" is under appreciated.

#### **B. FISMA Solutions: Expanding the 8570 Defense Department Initiative**

As the Subcommittee considers amending FISMA to enhance the security of federal systems, your attention is directed to a very successful Department of Defense (DoD) IT initiative. The DoD has raised the bar for cybersecurity through a training and testing program, commonly known as the 8570 Directive. This initiative focuses on the certification of personnel. Based upon my own experience in this industry, I believe that accreditations and certifications offer many benefits, including lower transaction costs. This year, my own IT business, Jenaly Technology Group, became the first in the country to be accredited for best practices in information security.

Remarkably, throughout the federal government, only the DoD has formally required its employees and contractors to get certified. In August 2004, the DoD issued Directive 8570.1. These groundbreaking guidelines recognized that awareness training and casual contacts with security

---

<sup>4</sup> See <http://www.comptia.org/sections/research/reports/200903-EUTSummary.aspx>

CompTIA  
FISMA Testimony  
May 2009

organizations were insufficient. In establishing this program, the DoD surveyed its IT workforce, assessed its requirements, and created three tiers of industry certifications based on whether the worker was a technical or managerial employee.

According to George Bieber, Deputy Director of Information Assurance (IA) Human Resources and Training at the Pentagon:

*The ultimate vision of Directive 8570.1 is a sustained, professional IA workforce with the knowledge and skills to effectively secure our enterprise information systems. This effort will enable DoD to put the right people with the right skills in the right places, and it's a tremendous opportunity for personnel to get the training they need to keep current with security in a continuously changing technology environment.*

The Congress should properly recognize the successes of 8570.1, which provides transparent, uniform and verifiable *industry-led* IT security compliance program for the Pentagon and its suppliers. Accordingly, it is recommended that FISMA be amended to clarify that "security awareness training" must also involve the testing and certification that personnel are properly trained.

Regrettably, this latest data shows that the civilian agencies are far behind the rigorous approach taken by the military. It is recommended that to enhance the IT security throughout the federal government, all federal agencies must adopt and implement the DoD 8570 model to expand training and testing.

Another reason for industry-based federal IT standards is the uniformity provided. Currently, many states, including the Commonwealth of Massachusetts, are prescribing certain new regulatory framework to reduce data breaches. Any effective national, federal security standard should be uniform and effective; in contrast, the prospect of 50 different state cybersecurity regimes poses significant problems for the small business community, including raising questions about its effectiveness and cost. A national, federal, regime akin to DoD's 8570 would set a uniform benchmark for agencies to meet, reducing complexity and administrative waste. The federal government should set a standard that could lead the country.

### **Conclusion**

In conclusion, it is undisputed that we must protect the American public by having a security framework that guards information systems for both our federal critical systems, as well as, the private sector. The computing industry is hard at work facing the unprecedented challenges of securing our data from both malicious threats and human error. Congress' enactment of FISMA has provided a base level of protection. The key to securing our systems for the future lies in the partnership between technology and human capital. By effectively managing both technology and people in concert, through training and testing (such as through the certification process), we can win the battles in the security war. The current Defense Department model surrounding the 8570 directive is a model worthy for emulation throughout the federal government. Any modification of FISMA must recognize the lessons surrounding the human

CompTIA  
FISMA Testimony  
May 2009

capital contribution to the IT security equation by the certification and accreditations to enhance our security.

Ms. WATSON. Thank you, Mr. Shoer, and thank all of the witnesses today.

We are now going to move to the question period and proceed under the 5-minute rule. I will open up the questioning.

I would like to start with Mr. Kundra. Your testimony specifically mentions that FISMA does not provide the necessary performance information to determine the Government's information security posture. So please cite for us what types of information it doesn't have, and how FISMA needs to be more reflective for the compliance requirements. Would you provide that information?

Mr. KUNDRA. Part of the debate is, as more and more transactions have moved to the digital world, if you look at legislation in general, or standards overall, the challenge is keeping up with the evolving threat. Because what ends up happening is, when you set X number of standards in terms of making sure reports are filed, whether that is annually or on a quarterly basis, it doesn't necessarily reflect your security posture.

An example would be within an agency, the old model used to be that you would build perimeter security in terms of firewalls. Because those threats were seen as, you had an enterprise and you had malicious actors on the outside that were trying to penetrate the defense that you had put in. So essentially, building walls around the agency.

But unfortunately, the malicious actors become more and more sophisticated in terms of being able to penetrate much deeper into the security systems. So now, being able to look at specific data elements and looking at the data itself, and you have this evolution, this race toward where you have actors that are actually going out there and making sure that they are able to bring down defense, whether they be firewalled, intrusion detection systems, intrusion prevention systems.

What we need to do is we need to be able to at the Federal Government monitor agencies more on a real time basis rather than on an annual or quarterly basis. We no longer can use a model that may have succeeded in an industrial era and apply it to the information age. Because we are moving toward a real time model where transactions and billions of dollars and information is moved on a real time basis. And therefore, we have to ensure that the metrics we are looking at move us in that direction.

Ms. WATSON. Thank you.

As part of this fiscal year 2010 proposal, the Obama administration is proposing to expand the use of its IT services, such as cloud computing and other types of data warehousing, software platforms, for managing agency data and systems. So I have a couple of questions on this.

What are the policies and protocols in place to ensure that the service providers and vendors are meeting information security and privacy standards set under FISMA and the Privacy Act?

Mr. KUNDRA. As a part of what we are making sure with the Federal CIO counsel is actually to ensure that FISMA is applied to any solutions when it comes to cloud computing. Second, from a philosophical perspective, what we need to make sure of is that security is actually baked into the very architectures of any solution, whether that is from a technical perspective or whether that

is from a cultural or human capital perspective. As shifts move in the industry toward cloud computing, it is not only important to bake security into the architecture, but also from a privacy perspective, but also from a privacy perspective, the CIO counsel has a privacy committee that looks at these issues.

And in conversation that we are having with industry, we are making sure that privacy issues and security issues are at the forefront and that they are also baked in early into the procurement cycle rather than afterwards, after you have procured a system, and then you have to go back and figure out what you need to do in terms of security.

Ms. WATSON. Is it fair to say that the companies providing these services to agencies ought to be responsible for providing at least the same information security protections that would be required of agencies who manage the data in house?

Mr. KUNDRA. I think what we need to make sure is that we look at it from a risk-based approach, which is, there isn't going to be one model that applies to everything. So there are classes of risk. What I mean by that is there is a set of services that the Federal Government has, which is public information, for example, that is not sensitive in nature.

So what you want to make sure is that you don't drive up the cost significantly for services that are not sensitive in nature and it is informational, versus having information that is either classified or sensitive in nature, where you need to ensure that the contractor or any company providing those services have baked in security. Our view would be, FISMA should be, as we look at standards, and as we look at technology, it shouldn't be seen as just a ceiling. It should be seen as the floor, but bake in even more security, depending on what the threat matrix is.

Ms. WATSON. Does anyone else, DOT, DHS, want to respond?

Mr. WILSHUSEN. If I may, Madam Chairwoman, a couple of points I would just like to point out. With services such as cloud computing or software as a service, it is, as Mr. Kundra mentioned, very important that the contracts and the organizations providing the services have adequate security mechanisms in place to provide the same level of security as needed and as required by Federal policy, since this is Federal information that is at risk.

One of the things that has been shown with this year's report is that the number of IGs who reported that their agencies almost always ensure that their contractors provide the same level of security required by FISMA, OMB policies and NIST guidelines dropped significantly at the same time that the number of contractor systems increased. So what happened is increasing reliance on contractors, where at the same time the oversight of those contractors is declining, as indicated in these reports.

So it is important that as these technologies and services come to the play, and are being used increasing by Federal agencies, that they do in fact assess the risks of using them and take the appropriate measures to make sure that the security controls are implemented and that the contractors are in fact providing the level of security required.

Ms. WATSON. Is there any other? Ms. Patillo.

Ms. PATILLO. Yes, if I may, Madam Chairwoman, comment on that question. I agree with Mr. Kundra that what we have to do is look toward risk-based systems, especially in our FISMA process.

What I would like to add new to that comment is, I believe that there has to be an integration with the capital planning process and FISMA. Currently, we sometimes look at that as two separate entities. At the Department of Transportation, we have one of the largest IT budgets in Federal Government, it is \$2.9 billion. Currently, I am spending \$125 million on security, which is less than one half percent on security.

So one would ask, is that the appropriate amount of dollars to be spending? We grapple with that from day to day. Is it accurate? Should it be more? Should it be less? Where should we apply it? Should it be toward certification and accreditation? Or should it be more toward contingency planning?

I think that with the integration of security and capital planning, we would be able to answer more questions and be able to apply more of a risk-based system.

Ms. WATSON. My time is up and we will come back to this in a minute.

I would like now to recognize our ranking member, Mr. Bilbray for 5 minutes.

Mr. BILBRAY. Thank you, Madam Chair.

When I see the defensive mechanisms [indiscernible] that is on, OK. Interesting that two of our mics went out. [Laughter.]

My staff always tells me, you are not paranoid, everybody really is against you. [Laughter.]

But we have been talking the defensive side. What is the ability for technology to find an electronic fingerprint of those who are probing our systems?

Mr. CHUN. Very little to nothing. The Internet was invented and developed with the complete assumption that everyone on the Internet would be a trusted source. So decades ago when it was actually developed, there was no real concern or thought over someone on the Internet would need to be traceable, and No. 2, would actually have ill intent.

So I would guess the answer, I think the question you are alluding to is attribution, can we attribute these attacks definitively to a source. I believe the current infrastructure technology answer is no, or very difficult.

Mr. BILBRAY. Are we working on technology to be able to track sources?

Mr. CHUN. The industry itself is looking at modifying the basic framework of the Internet. Very complex issue. There are interoperability issues with older networks and systems. But there are various organizations, including the ones that are sponsored by the Government, such as DARPA, that are looking into these fundamental issues of how do we change the Internet into something more trustworthy. And that is a very complex, long-term effort. I can't speak for everyone at Hewlett-Packard, but I personally believe this is more of a generational issue than one that we can fix practically very quickly.

Mr. BILBRAY. I have to assume, there are always those that assume that anonymity is a great thing, the Government, no one

should be able to track whatever I do on the Internet. Though we take it for granted that we have caller i.d. with our phones. I am sure this has the black helicopter people looking at this as some great conspiracy by Big Brother.

But I darned well think that it is absurd that we have to play constant defensive ball here and not be able to spend some of those resources at tracking down who is probing, who is prodding, who is trying to find a weak spot. There is no defensive system in the world that can handle constant bombardment of those kind of probes without a weak link being found somewhere down the line.

I know in 1996, Madam Chair, when I was serving on Energy and Commerce and we were looking at the telecommunication forum, user i.d. was always a big issue, not just for security reasons, but for the interstate gambling aspect of it, the consumption of alcohol, tobacco, pornography, there was all this stuff. I think that we really have to be very frank and open about the fact that this user i.d. is something that needs to be followed up on. It may be one of those things that we want to spend more money on being able to track down.

God knows, every one of us watches CSI and sees what we have done with tracking down bad guys electronically. Maybe we need to be looking at some of this technology in the future.

So that really concerns me. What do we have right now as a strategy to go after the bad guys who are probing? Or is it the fact that we don't have a way of tracking, so we just accept that we can't do that?

Mr. KUNDRA. No, we are actually, the Department of Homeland Security, and I will defer to Ms. Graves here, but US-CERT monitors the Federal infrastructure to be able to respond accordingly. And on research and development, investments are being made, whether it is through the National Science Foundation or whether it is with DARPA, and of course, working closely with the National Security Agency, to look at what the security and the threat matrix is.

But you are absolutely right, in terms of the nature of the threat, it is constantly evolving, as actors go up, as you stand up defense systems, making sure that there are actors out there who are also making the appropriate investments to be able to penetrate those defense systems. So we have to be ever-vigilant, and it cuts across through everything, through the culture of an organization, the human capital and even the technology systems that are out there.

Mr. BILBRAY. Ms. Graves.

Ms. GRAVES. Yes. To further comment on the US-CERT capability, we do have these Einstein sensors that are located in the Federal Government now, and they have signatures and scripts for people who specifically target the Federal Government. Once an intrusion is determined to be active, we open cases and we do the forensics on those particular cases, scans, and we do track back to the original source. That does take time. There is no efficient technology to do it. But we do have individuals in place from an intelligence community perspective who deal with these types of threats who aid us in that forensic analysis.

Subject to future capability, we will also be adding to that in the Department of Homeland Security in terms of the cybersecurity ini-

tiative and plussing up the capability that we have in US-CERT and also in NPPD. But that is human. That is the human side of following the threat, of doing the analysis, of determining the source and of looking at counter-intelligence measures and reasons why these specific people are targeting the Government.

Mr. BILBRAY. Madam Chair, I think this is something that both sides of the aisle need to be brave enough to address. There are people on the left and the right who would not want this technology. But it is not just a national security issue. It is the security of our children, and everybody knows the predator issue. It is sad that we need to have a television show set up sting operators for predators, because we don't have the ability to really trace these down.

I just look forward to the day that we can literally have some of these probers drawn and quartered in the public square to basically send the signal to everybody, especially our children, that this is not something that is acceptable in a civilized society. Though drawing and quartering is. [Laughter.]

I yield back.

Ms. WATSON. Thank you.

Mr. Connolly.

Mr. CONNOLLY. Thank you, Madam Chair.

Hopefully I can be heard. Thank you, Madam Chairman.

[Remarks off mic.]

Ms. WATSON. Sorry about these mics.

Excuse us. You see we need your technology.

Mr. CONNOLLY. Madam Chairman, I would ask unanimous consent that my statement be entered into the record as read, given the fact that it could not be heard. [Laughter.]

Ms. WATSON. Without objection.

Mr. CONNOLLY. Madam Chairman, one of the concerns I have about this subject is how we are coordinating at the Federal Government level. And I have introduced a bill to try to codify by statute the Executive order issued by the President to create a CTO position. The good news is, we have two highly qualified people, Mr. Kundra and Mr. Aneesh Chopra. But when we look out to the future, we are not always going to have an Obama administration in place. I believe very, very strongly that we have to have a statutory framework that delineates the respective responsibilities between the two.

I would hope, Mr. Kundra, that you would take that message back to the White House. Because we need to work together. There are some changes that need to be made in the legislation, fine. But I believe, Madam Chairwoman, we have to address this issue, this committee has to address that issue on a statutory basis. I certainly intend to proceed with the legislation. I would like to have White House input in doing that. And I thank you.

Mr. Chun, you talked in your statement about governance as the first challenge. You said that we need a new and empowered leader to spearhead the effort. What did you have in mind?

Mr. CHUN. Someone that we can go to directly. For example, if there are issues with some of our contracts, we are almost always going directly to a specific person at that agency. While that is

good, I think as an industry as a whole, we need literally an office we can go to for a coordinated effort.

We participate in lots of industry activities, BSA, which is a software alliance, Tech America, all those venues. When we talk to our partners, we hear pretty much the same thing from industry and a corporate level, is there someone that is central to the Government that is in charge of these particular issues, someone that I think would be valuable to us.

Does that answer your question?

Mr. CONNOLLY. I think it does, but I think you are talking about on an agency by agency basis.

Mr. CHUN. No, I meant that as what we do from a business standpoint. But when that industry engages, such as the technology industry engages as a whole, there appears to be a lot of companies that belong to an organization that deal with a specific agency question or something that specific department may issue a question. And until very recently, when the cybersecurity review was being performed, we haven't seen one from a central office in Government that says, we need your input. I think that is a really critical thing that has been a positive for us.

Mr. CONNOLLY. Well, hopefully the creation of a CTO may help us with that. I think that is worth monitoring carefully.

Mr. Kundra, in your initial review of information security, you referred to the FISMA requirements as cumbersome and labor-intensive. I wonder if you could give some examples of how we could improve the process from your point of view.

Mr. KUNDRA. Sure. Part of what we need to be able to do is, from an OMB perspective, automate a lot of the reporting in terms of collecting information. Second, is we need to be able to rationalize as far as which metrics we are going after, which ones are important and which one are not. Having thousands of metrics doesn't necessarily add value unless those metrics are relevant, those metrics are able to respond to the real time threat and the nature of the threat that we face, and are evolutionary in nature in terms of recognizing that as we put up defenses on the other side, there are people putting up offenses.

So how do we measure metrics, or how do we look at and approach security for a position that it has to be one baked into the architecture, whether it is system, agencies, culture? Second, how do we make sure that there isn't a model of faceless accountability, that we are all accountable when it comes to information security and the management of those security systems? Third, how do we move toward an area where we are actually monitoring, similar to what US-CERT is doing, across the board on a real time basis as threats emerge, so we can see from a leading perspective which threats are emerging across the world, so that we can be beneficiaries to ensure that we are putting up the proper defenses in an ongoing basis?

Mr. CONNOLLY. Thank you.

Mr. Wilshusen, Government often likes to do that which it can measure most easily. Cybersecurity, educational awareness is measurable. We trained 400 people this week. Check. The question really is, but are we in fact more secure today than since we passed FISMA, with the best of intentions. And perhaps one can draw the

inference from the GAO report that the answer to that is more problematic than we want to admit. What is your comment?

Mr. WILSHUSEN. Well, I would certainly say I agree with your comment that what gets measured pretty much gets done. And one of the areas that we can do, have additional improvements, as Mr. Kundra mentioned, is in the type of measurements and the measures that we actually use to monitor the security at the agencies.

As we commented before, many of the measures that are presently being used are basically compliance-related, implementation measures. They don't measure how effective an agency is in actually implementing a control. And so that is one of the areas where we need some improvement.

And certainly the measures that are currently being used are in fact defined by OMB. So Mr. Kundra and OMB is in a good position then to make changes to that particular mechanism for monitoring security.

But indeed, the Federal agencies have spent a lot of money trying to secure their systems and complying with various different requirements. It is still very much an open question whether we are more secure.

I would say that with the evolving threats, and with the new, emerging technologies that are in place, as well as the changing business practices, they all increase risk to Federal systems and operations. It is a very fluid, dynamic environment that we have to address on a regular, real time basis.

Mr. CONNOLLY. Madam Chairman, I am sure my time is up, but I want to suggest that we may want to invite our Federal witnesses to provide the subcommittee with their recommendations for how we might improve FISMA toward the goal of ensuring cybersecurity. I am far less concerned about how many people we train in awareness, though that is important. But the goal isn't awareness, that is part of the process. The goal is to ensure the security of the system.

And frankly, Madam Chairman, I am so glad you are having this hearing, because frankly, if people really looked at the potential threat, we would have to have this hearing in the Cannon Caucus Room in terms of its importance. I want to thank you again for holding this hearing, because I can't think of a topic that is more timely and more important as we look out to the future.

Thank you.

Ms. WATSON. Thank you.

The GAO reports that many of the Government data losses were a result of physical theft or improper safeguarding of systems, including laptops and other portable devices. I recall the well-publicized event several years ago of a computer that was stolen from the Veterans Affairs employee with a massive amount of personal data of the VA beneficiaries.

How many of the reported security incidents are considered physical breaches as opposed to data that is lost or corrupted through cyber means, and what additional security vulnerabilities do cell phone and BlackBerrys and other wireless devices present to securing sensitive or classified information?

Mr. WILSHUSEN. I will start off, if you don't mind, Madam Chairwoman.

With regard to the actual number of incidents that have been attributed to physical security lapses, such as theft or loss of laptops, I don't have that specific information. The information that is presented in agencies' reports to the US-CERT has shown that the number of total incidents has tripled over the last 2 years, from 2006 through 2008. And of that, the physical security portion of that would be one of the categories that is included in the unauthorized access category that US-CERT requires agencies to report under.

Of that, there is about 18 percent of the number of incidents that occurred, triple, from 5,500 in 2006 to over 16,000 in 2008. About 18 percent of those related to unauthorized access to information. That would include both cyber access, where someone came in through a network and was able to access information, as well as those pertaining to the loss or theft of a laptop or some other physical means.

But certainly, that is a key control threat and vulnerability of Federal systems, is the fact that so much of the Federal work force is mobile. The data is becoming increasingly portable through not just the laptop computers, but also thumb drives. It is important that appropriate security measures, such as encryption and other capabilities, are installed to help mitigate the threat of such incidents occurring.

Ms. WATSON. Can we mitigate those threats?

Mr. WILSHUSEN. We can certainly try to address them and take appropriate controls to help reduce the risks associated with those threats. I guess it is also important to realize that risk avoidance is not even a goal relating to cybersecurity, it is managing the risk. So we have to assess the risk with the information, first of all, as Mr. Kundra mentioned earlier, is this information sensitive and from what purpose, from a confidentiality perspective or integrity. And then if it is not sensitive from a confidentiality perspective, then the level of controls might be less than if it is sensitive information and then we may want to use encryption. For example, personally identifiable information, OMB has issued policies in the past requiring that agencies that put sensitive information on their laptops be encrypted, and that the life of that information on that laptop be limited to 90 days and then it should be reevaluated, whether that information should continue to reside on that laptop.

So there are controls that could be in place and in fact are in place at some agencies. But they probably need to be implemented on a more regular basis.

Ms. WATSON. How can we harmonize across these agencies? What I see is that each agency has different standards. So some way we need to coordinate and harmonize. How can we do that?  
Mr. Shoer.

Mr. SHOER. Madam Chair, I think you are touching on something that I commented on in both my oral and written testimony. If I can try and distill what you are saying into my own words, the technology exists to address the various issues and threats that you are speaking about. But what often gets lost in these discussions is that the human being, you and I, are still, despite all the technology, we are still the last line of defense. I see this in the private sector as well as the public.

The bottom line is we feel very strongly that it is only through a level beyond awareness training, as you pointed out, the awareness training is wonderful, but it is documented to be insufficient. We need to be pushing training down from the IT staffer level throughout the agencies to ensure that those who have access to this sensitive information are clearly trained and certified in their ability to have access to it and use it.

Ms. WATSON. I will yield to Mr. Bilbray.

Mr. BILBRAY. Let me followup on a different line here. The discussion of bringing in basically an IT security expert into the White House, will that help coordinate the efforts or basically just add another layer?

Mr. KUNDRA. That has been part of the 60-day review, working with Melissa Hathaway, looking at how we are organized across the board within the Federal Government. At the same time, we recognize that cybersecurity is such a vital issue and it cuts across every aspect of life when it comes to the Federal Government that we need to ensure that we have the proper attention and that the President's recommendations are going to be forthcoming in terms of the 60-day review, in terms of what we need to do to ensure that we are organized in a way that allows us to respond to these evolving threats.

Mr. WILSHUSEN. And if I may add, Ranking Member Bilbray, GAO convened a panel of cybersecurity experts a couple of months ago to look at that very same issue and to provide recommendations or suggestions for improvement into the National Cybersecurity Strategy. And they suggested that, indeed, establishing White House responsibility and accountability for leading and overseeing national cybersecurity policy is very important.

One of the problems that has occurred to date in this phase is that much of that responsibility has been given to DHS in its role. But for a number of different reasons, including the turnover of key personnel, and the fact that they didn't have authority to monitor budgets or anything like that, they had limited effectiveness in performing that role. So elevating it up to the White House was one of the issues that our panel of cybersecurity experts felt was needed in this respect.

Mr. BILBRAY. So you do support it?

Mr. WILSHUSEN. Yes.

Mr. BILBRAY. What does that do to the oversight jurisdiction of this committee and the other committees in the House and Senate?

Mr. WILSHUSEN. I don't know what the specific impact would be by elevating that with regard to the oversight of this committee.

Mr. BILBRAY. While I have you here, there was testimony here about the DOD's directive in the initiative to ensure and require certification. Do you think this is a program that we should use as a model or do you see major shortfalls here, are there shortcomings of the concepts, or do you think we have operational systems that are just as good?

Mr. WILSHUSEN. I think any time you can improve the skills, knowledge and abilities of those individuals responsible for implementing security, it is a benefit. The key, as I mentioned earlier, was the fact of providing computer security awareness training, while that is fine, it still gets to the point of how effective is that

training and how will we know whether or not individuals responsible for implementing security actually act appropriately in the time and deed when they are being challenged.

That is why having measures as the number of personnel that might be certified or that have received computer security awareness training may be somewhat misleading. What would probably be a better measure is to have some sort of a challenge response test to see how they react when an incident occurs. And just as an example, the Internal Revenue Services has a pretty good program of where the IG would actually ask specific questions to their claims representatives over the phone about a tax question, and then they could then determine how accurate those responses were and whether or not they were getting accurate tax information in response.

Mr. BILBRAY. My father has been in the tax business since the year I was born, and believe me—

Mr. WILSHUSEN. And what they typically find is that many of the responses they receive from their tax representatives are wrong and incorrect. Why can't we design similar tests for cybersecurity? Why can't we send perhaps an email to an individual to see how many of them actually open up the attachment or click on a link?

Mr. BILBRAY. We don't do testing systems right now?

Mr. WILSHUSEN. We test systems, I don't know if we test the effectiveness of those systems across the board. Certainly we don't do that as part of the FISMA reporting process.

Mr. BILBRAY. Madam Chairman, you remember, this is something we probably need to talk about too, is they just did a test to see about getting passports and phony i.d. and four out of four, bam, right through. That is a whole different issue.

After the mics have been all messed up all day, I am in a paranoid sense here. But how do we know that the people we are hiring aren't working for the bad guys? What kind of security does DOD do when we bring people on? How do we know? Do we use biometrics? Do we do background checks? How do we know the bad guys aren't slipping into the system and actually programming our systems?

Mr. SHOER. Thank you, Ranking Member Bilbray. I can't speak specifically to that, but I can certainly find the answer for you. But I can tell you that in some of the private sector equivalents that CompTIA is involved in, and CompTIA was intimately involved in the 8570 Directive, those controls are there. Background checks are a critical piece of that accreditation.

So those controls are there. I think to your earlier question about the type of testing that goes on, there is a testing component to 8570, but again, I will have someone get back to you in writing with the specifics on exactly how far that goes, so that you know how applicable that model may be to the rest of the Government. We think it is very applicable.

Mr. BILBRAY. Right now, employees all go through at least E-Verify to make sure their Social Security Number and their names matches, right?

Mr. SHOER. I would think at a minimum.

Mr. BILBRAY. OK. But the contractors, the administration has, the previous administration and this administration, has delayed

the E-Verify requirement for contractors generically from February now or late June. Hopefully we will see a go. But the fact is that right now, in the IT system, do we use that on contractors who are brought in to do work? Everything is in-house.

Mr. SHOER. One of the things you might want to investigate, and without getting too far off track, the Commonwealth of Massachusetts, as you may know, has passed some fairly sweeping information security privacy regulations. Part of that is certifying that the third party vendors that are hired, now this is focused mostly at private sector, but again, I think ultimately there is a tremendous opportunity for a public-private partnership here in sort of establishing these standards that will work throughout the Federal system as well as the private sector.

But you will have to, for example, as a very simplistic example, you mentioned tax work. So if you are a CPA firm and you engage a company like my own, a VAR, to work with your information systems, we have to provide that safe harbor information that certifies that we have done all the things you are talking about so that organization knows that the contractors they are bringing in meet these various stringent requirements.

I think something similar at the Federal level makes perfect sense.

Ms. WATSON. Thank you for that.

Senators Rockefeller and Snowe recently introduced legislation that included provisions to establish a cybersecurity office in the White House, along with Federal acquisition and procurement requirements for IT. I would welcome in writing your comments on what should go into the legislation.

There is a draft out now. But you just might want to suggest what should be included in that legislation. Several Members have mentioned, we will probably need some kind of policy to deal with this. So I would like to have your input as well.

Now, moving on, the GAO reported that 23 of the 24 major agencies for fiscal year 2008 did not identify or authenticate users in order to prevent unauthorized access to agency networks. Authenticating users appears to be a fundamental security breach at the front end that can have a cascading effect on security breaches throughout the system. I know you, Mr. Bilbray, raised this issue during our last hearing.

Do we know who is authorized to have access and who is legitimate and who is not? Why have the vast majority of agencies failed to create adequate security measure to identify and authenticate users? This question has been raised, but I would like to hear further comment from you on why it is taking so long to do this. Mr. Chun.

Mr. CHUN. I believe the agencies that have complied, the ones that come to mind are the Defense Department, and the Marine Corps, under that contract.

Ms. WATSON. The GAO said 23 of the 24 major agencies did not identify.

Mr. CHUN. There are agencies, I was alluding to, trying to relate a success story, for bringing the Marine Corps into that contract. We were one of the first to implement a cryptographic log-on mandate, which basically says you need to use multi-factor authentica-

tion. You use what you are, what you have, instead of just typing a user and password in. The technology does exist. It has been implemented and has been successful in other places. I can't speak for the specific reason why an agency would choose or hasn't gotten to that.

But it is relatively mature. Matter of fact, it doesn't necessarily need to be two, there could be many multi-authentication factors to gain access to a system. But you do have to balance, and it is always kind of a sensitive thing, what security is. The safest computer in the world is one that is not connected to the Internet, in a steel bunker with no windows and no doors. [Laughter.]

You can put so many controls into a system that it is actually not providing any value to the mission of the agency. So it is one of those things that we try to be particular about. That is one that the technology exists, it is mature, we believe, and has been used in the past. So we encourage all the agencies to look at that.

Mr. BILBRAY. Madam Chairman, would you yield, please?

Ms. WATSON. Yes, Mr. Bilbray.

Mr. BILBRAY. Does the DOD now use any biometrics to confirm? Or is it all strictly just on data information?

Mr. CHUN. I can get you the specific technical details in written form. But the common access cards they use, it is capable of storing biometric information. Whether that is used specifically, I will get back to you on the cost to DOD. And maybe you can ask a better question of the Defense Department. Matter of fact, I believe they do use biometrics on their cards.

Mr. BILBRAY. I always bring that up, Madam Chair, I don't know if you use the CLEAR system when you fly back and forth to Los Angeles, but there is a system that has multiple checks, so it rotates stuff around. It is probably going to, in a lot of ways, be this sort of flagship of indication of what is possible with a whole lot of these issues.

I yield back, Madam Chair.

Mr. WILSHUSEN. Madam Chairwoman, if I might just clarify one point.

Ms. WATSON. Yes.

Mr. WILSHUSEN. What we have found is that 23 out of 24 agencies did not sufficiently implement controls to effectively prevent, limit or detect unauthorized access to systems. So it is a little bit broader than just identification and authentication controls. But it also includes weaknesses related to boundary protection, making sure that firewalls and routers are adequately configured, as well as the authorization controls, which assure that agencies only grant the level of access to an individual necessary to perform that individual's job and no more.

It also includes their procedures for auditing and monitoring access to that work, looking for intrusions and the audit and logging capabilities, as well as physical security to computing resources. So it is a little bit broader than just those controls used to identify and authenticate the identity of users.

Ms. WATSON. We hear from these agencies that it is under review. Is it that we are short-staffed, or the expertise needs to be increased? Or do we lack the resources, financial resources, to speed it up?

Mr. WILSHUSEN. I think it is probably——

Ms. WATSON. All the above?

Mr. WILSHUSEN. Probably so. One of the things that is important to understand is that many of these capabilities already reside in the systems at hand, that are in use. So it is important upon agencies to actually implement and configure the systems accordingly to provide the level of security that is required to protect their information systems.

Ms. WATSON. Do you feel it is the lack of oversight from the policymakers or, there is new technology being developed every single day, and getting the handle on how we secure it to reduce the risks and the vulnerabilities of that system, it is mind-boggling. Anyone who wants to comment, please do.

What we are going to do, as a subcommittee, is provide information from the testimony that we have up to the full committee for policy. So just break in at any time, because we want to get this right from the beginning, if that is possible. Ms. Patillo.

Ms. PATILLO. Yes, Madam Chairwoman, I would like to comment on that. At the Department of Transportation, we look at the amount of events that are captured through our cybersecurity management center. When we look at those, it is mind-boggling, if you would realize that there are 3 million events that come in on a given day.

Of those 3 million events, we have to analyze those into actionable events. What we typically come up with at the end of the day out of those 3 million is 10 actionable events. So there is human intervention among analyzing that. So if one could just try to visualize individuals that are having to correlate this data to figure out which are really actionable events, we find that, what I believe, as Mr. Kundra has said, we have to look more to automation and the technology. Because if you are looking solely to human intervention to analyze what this means that comes into our networks on a given day, wouldn't it be simpler if we had an automated way of determining which events are actual incidents?

Mr. KUNDRRA. If I could add to that, it is also looking at the default setting of products and services that the Federal Government procures. From a commercial perspective, what a lot of the providers want to do is they want to have maximum functionality and they want to make available as many options as possible. Unfortunately, a lot of those options end up causing vulnerabilities in the systems themselves.

So if we think of it on the front end, in terms of making sure that the default position, when it comes to whether it is systems the way they are configured or it is services that we are acquiring, are as secure as possible, and then one by one, based the options we need, we would turn them on, I think it moves the security agenda much further forward.

Ms. WATSON. I want to go back to you, Ms. Patillo. You have all these actionable items. What would you suggest that we put into policy that will help, since you have these incidents 100 times a day, what would you suggest that we do policy-wise that will assist you?

Ms. PATILLO. From a policy perspective, what could assist us, I believe, as Mr. Kundra has already articulated, we need to look at

the very beginning of the process which begins with procurement. At the onset, all contracts should be required to have security baked in at the very beginning.

Ms. WATSON. Should we do that through policy, or can you do that within your own department, for that requirement?

Ms. PATILLO. We could do that within our own department, but I believe that it gives it an extra sense of authority if perhaps we could have it written in the FAR.

Ms. WATSON. OK.

Mr. Kundra, did you want to address that?

Mr. KUNDRA. No.

Ms. WATSON. Mr. Shoer.

Mr. SHOER. I think we have seen some advances in the acquisition process. I believe, I can double check, I think this is actually written into the Federal Acquisition Regulations, a specific section about security that wasn't there before. We are also seeing a lot more security as a requirement, a clear, articulated requirement in acquisitions that we respond to. So I think those are some very positive steps forward.

I am not entirely convinced or sure, whether at a policy level, how that interacts with actual tactical acquisitions that go out. But certainly it is something that has been done, we support it, especially if it is very clearly articulated, so we can meet it. But at a policy standpoint, I just don't see how that would be connected from a policy level other than being to make this not quite this way. Does that make sense?

Ms. WATSON. Somewhat. [Laughter.]

We ourselves are trying to reach for solutions to mitigate some of these issues. So we expect you as the experts to suggest to us. So really what I would like you to do, we are going to be addressing these areas that we have been focusing on today. Put in writing your recommendations, and we will see what we really need to add to what is already in the law. And if we can improve it, we will. So just feel free to recommend to us.

Mr. Wilshusen.

Mr. WILSHUSEN. One thing I might add, and it is expanding what Mr. Kundra said, is one of the areas that we should probably look at is instead of looking at acquisitions on a department by department level, is looking at it on a Government-wide basis. Because the Federal Government spends billions of dollars, I think it is like \$70 billion in IT products and services for its fiscal year, is to leverage the procurement power of the Federal Government collectively to achieve both cost savings and to help incentivize the vendors and the producers of this offer to provide or secure products. There are a couple of initiatives already underway through SmartBuy that GSA has which helps to allow agencies to buy encrypted products at reduced rates and at cost savings, as well as the Federal desktop configuration, which Mr. Kundra alluded to, in terms of having the vendors products with security already built into it.

Ms. WATSON. Thank you.

We are going to conclude this, but I would like Mr. Bilbray to followup.

Mr. BILBRAY. Yes, let me followup on that. Madam Chair, the conversation just really went to the road map of where we need to go down the line. Those of us in California, in the 6-years I served on the Air Resources Board there, there was a thing called technology-forcing regulation that traded the cleanest fuel, cleanest cars and really pushed it.

But one of the things I am really upset about, what I am seeing come out of Energy and Commerce right now, or what was announced today of a standard that the Federal Government was going to set for everybody else, but not using our procurement resources as a way of leading through example, I think that a lot of us on both sides of the aisle feel that if the Federal Government had led through example of buying clean energy for this facility, going out and buying high efficiency vehicles or ordering massive amounts over a period of years, that would create the incentive and the market for the research, development for the kind of product we want to see.

We have been able to do that in California by setting goals that were over the horizon but within the realm of reality. And the private sector, because of the profit incentive, has been able to develop technologies that we desire to possess somewhere in the near future.

So I guess the issue here is, the Federal Government can lead through example by using those huge resources to be able to develop that. Then the spinoff goes over to the private sector where they then can benefit from that technological breakthrough.

Ms. WATSON. With that, we are going to have to conclude this hearing, we do have a vote out.

I want to thank the witnesses for your testimony today. We consider you the experts, so as I suggested before, we would appreciate your writing your recommendations. We will continue down this road, because we have the responsibility of looking at procurement policies. So this is a work in process. And we are going to try to refine it, each time we have a hearing.

We don't know it all and we haven't heard it all. But I think this hearing was very valuable. I hope the recorder was able to get everything down, because there has been a lot of good information offered. We will see next time we hold a hearing that our systems work. [Laughter.]

But with that, I want to thank you for attending, your testimony, the audience for being good listeners, and the ranking member, Mr. Bilbray, for your insights.

With that, this hearing is adjourned.

[Whereupon, at 11:10 a.m., the subcommittee was adjourned.]

