AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

FEDERAL INFORMATION SECURITY: CURRENT CHALLENGES AND FUTURE POLICY CONSIDERATIONS

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

SECOND SESSION

MARCH 24, 2010

Serial No. 111–145

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

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

U.S. GOVERNMENT PRINTING OFFICE

65–549 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON 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
JUDY CHU, California

DARRELL E. ISSA, California
DAN BURTON, Indiana
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
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
BLAINE LUETKEMEYER, Missouri
ANH "JOSEPH" CAO, Louisiana

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
MIKE QUIGLEY, Illinois

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

BERT HAMMOND, *Staff Director*

CONTENTS

FEDERAL INFORMATION SECURITY: CURRENT CHALLENGES AND FUTURE POLICY CONSIDERATIONS

WEDNESDAY, MARCH 24, 2010

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 2 p.m., in room 2154, Rayburn House Office Building, Hon. Diane E. Watson (chairwoman of the subcommittee) presiding.

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

Staff present: Bert Hammond, staff director; Valerie Van Buren, clerk; Adam Bordes and Deborah Mack, professional staff members; Charles Phillips, minority chief counsel for policy; and John Ohly, minority professional staff member.

Ms. WATSON. The Committee on Oversight and Government Reform will now come to order.

Today's hearing will review the Federal Information Security Act [FISMA] of 2002, and agency efforts to improve the security, integrity, and reliability of the Federal Government's information systems.

In addition, today's hearing will address legislation introduced by me last week to amend FISMA, H.R. 4900, the Federal Information Security Amendments Act of 2010.

I welcome all of our distinguished panelists and look forward to your testimony, and apologize for being late; we were in a very important meeting.

So, 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 other Member who seeks recognition.

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

Now, I would like to wish everyone here a good afternoon and welcome to the Government Management Subcommittee's oversight hearing on the state of Federal Information Security and agency efforts to comply with the Federal Information Security Management Act, and we will also discuss proposed legislation I recently introduced to amend FISMA, the Federal Information Security Amend-

ments Act of 2010. I look to our witnesses and your testimony, and we appreciate your presence here today.

Since enactment of FISMA legislation in 2002, this subcommittee has held annual oversight hearings on agency efforts to meet the standards and policies prescribed under the current FISMA framework. While some agencies have shown great success in harnessing both technology and human capital to reduce their overall cyber risk profiles, many others simply comply with the basic annual reviews and periodic assessments required under FISMA that reveal only a fraction of the threats and the vulnerabilities facing them.

It is clear that the notion of being in compliance with current law does not equal having adequate security across an agency's IT infrastructure. Furthermore, the vast majority of Federal agencies still have not met the basic cybersecurity requirements outlined in the FISMA legislation. According to statistics from GAO's testimony and OMB's annual FISMA report to Congress, 23 out of 24 agencies have been identified as having weaknesses in their agency-wide information security programs.

Although these figures do not speak to the depths of problems that agencies have, it tells us that many still view security as a measure of efficiency or productivity, and not as a pillar of necessity or national security. It also indicates that OMB has not used its enforcement authority and budget power to force agencies to make effective information security a fundamental requirement in their daily operations and strategic plans.

While some may view these problems as insurmountable, I believe there are managerial blueprints at some agencies that have proved effective in reducing their exposure to cyber threats. For example, the State Department has utilized a number of mechanisms, including stronger baseline internal controls, newly developed performance metrics, and advanced system monitoring capabilities for reducing their risk exposure by nearly 90 percent.

These outcomes are by no means perfect. But they underscore the ability of agencies to both prioritize the mitigation of their largest cyber vulnerabilities while working to meet the minimum security standards and policies prescribed for all of their IT assets.

So, as we move forward with policy goals for reforming FISMA, we must try not to look for a silver bullet as a solution for information security deficiencies, but to develop a harmonized policy framework that addresses our current managerial, planning, technological, and leadership shortcomings across the Government.

It is in response to these challenges and deficiencies that I have introduced H.R. 4900, the Federal Information Security Amendments Act of 2010. The bill before us is a combination of multiple policy recommendations and legislative proposals, including those from President Obama's recent cyberspace policy review, the CSI Commission on Cybersecurity for the 44th Presidency and the GAO. It includes a combination of visions to strengthen our managerial, our technical, and our strategic planning objectives while flexible enough for individual agencies to address their unique information security profiles.

The bill establishes a National Office for Cyberspace within the Executive Office of the President. The Director of the National Office for Cyberspace, appointed by the President and subjected to

Senate conformation, will be charged with overseeing the cybersecurity posture of the Federal Government. The Office's mission will be to develop and manage through an interagency board consisting of OMB, civilian, military, and other agencies that will oversee the crafting of policies and guidance that are responsive to combating the changing nature of cyber threats Government-wide.

I firmly believe the establishment of the National Office for Cyberspace will provide both the Presidential leadership and policy focus capabilities that are needed for addressing our cyber deficiencies Government-wide. The legislation also moves agencies away from the current paper-intensive process used to monitor agencies' compliance with FISMA policies and procedures and, instead, will require agencies to utilize automated technologies and outcome-based performance measures for determining their true cyber risk profile.

By utilizing new monitoring and measuring capabilities, agencies will have much more complete data at their disposal for mitigating their most significant vulnerabilities and combating future cyber threats.

Last, the bill requires OMB and agencies to inter-cooperate information security into their procurement decisions through secure acquisition requirements for commercial products and services, and vulnerability assessments for major information technology investments. I believe those provisions offer us the best way forward to ensure that information security is built into our agency systems in a technology-neutral manner from the beginning of the procurement life cycle.

In closing, I believe reducing our exposure to current and future cyber threats will require both managerial discipline and policy flexibility. While the legislation I offer is not perfect, I believe it provides us a way forward to reducing our cyber risks across the Government, while instilling policy leadership on cybersecurity at the highest levels of our Government.

Once again, I welcome our panelists today and I look forward to their testimony and their feedback.

At this point, I would like now to yield to our distinguished ranking minority member, Mr. Bilbray of California.

Mr. BILBRAY. Thank you, Madam Chair. Madam Chair, your opening statement was so well drafted and so comprehensive and so well delivered that I just ask for unanimous consent that my written statement be entered into the record.

Ms. WATSON. Without objection.

Mr. BILBRAY. And just quickly pointing out that this is quite an appropriate step that we move forward here. We are seeing that the cyber world is becoming not only a tool, but an essential foundation for the Federal Government's ability to perform our constitutional responsibilities. Everything from, now, employment verification to we are looking at the taxation system, the IRS's ability to use it has just been a huge boom. The security at our ports of entry to our military applications, to our health care service capability. All of these are going to expand extensively, and should, to be able to make sure the Federal Government is as effective and efficient and as cost-effective as possible.

Along with that great opportunity comes a huge threat, and I think that we will find that what you are doing here today, if we do this right and follow through with this appropriately, will not only be defending those components that we see today, but be actually creating a vehicle that will protect the future expansion, which will probably be tenfold of what we see today.

So, again, I appreciate the introduction of the bill. We will work at trying to improve it. Nothing is perfect, but we will darn well do our best to make sure that we create this defense shield as strong as possible. And I yield back, Madam Chair.

Ms. WATSON. Thank you.

I now yield to Mr. Connolly.

Mr. CONNOLLY. Thank you, Madam Chairman. I would ask my full statement be entered into the record.

Ms. WATSON. Without objection.

Mr. CONNOLLY. I thank the Chair.

If I could add one point, one of the concerns I have, among many, is that we get the architecture, the managerial architecture of cybersecurity and information technology in general in the Federal Government right. The President, by Executive order, has created a position of Chief Technology Office, which I applaud. I believe we have to, however, create a statutory framework for that position and the cybersecurity position as well. So making sure we understand, moving forward, in a statutory framework, beyond just an administrative framework, what those pieces are and what those responsibilities are, and how the org chart works I think is very important, given the resources we are going to be putting into these efforts.

So one of the things I certainly want to do—and I have introduced legislation, H.R. 1910—I have yet to hear from the administration on that bill, but I want to certainly incorporate elements of that into whatever we do by way of reauthorization of FISMA, and I intend to do just that.

Thank you, Madam Chairman.

[The prepared statement of Hon. Gerald E. Connolly follows:]

Opening Statement of Congressman Gerald E. Connolly

"Federal Information Security: Current Challenges and Future Policy Considerations"

Subcommittee on Government Management, Organization, and Procurement

March 24th, 2010

Thank you, Chairwoman Watson for holding this hearing on the Federal Information Security Management Act. As we prepare to reauthorize FISMA, I think we need to focus on two issues. First, we need to address federal organization of information and cybersecurity officers, including the CIO, CTO, and Cybersecurity Coordinator. Second, as the GAO and Vivek Kundra have explained at length, we need to transform a federal culture of compliance to a culture of cybersecurity performance.

I have introduced legislation entitled the Chief Technology Officer Act, H.R. 1910, which would make the Chief Technology Officer (CTO) a statutory position. Technology firms and federal contractors rely on effective, consistent technology policies and organization. In order to maintain the focus President Obama has placed on technology, we must make the CTO a position established by statute. When we make this position permanent, we also need to ensure that we have a rational federal organization of technology officials. Recently we have a renewed and justified interest in technology and cybersecurity, which spurred the creation of a CTO and Cybersecurity Coordinator. We have not done an adequate job establishing responsibilities and hierarchy among these positions and the Chief Information Officer (CIO), which preceded them. It would be logical to have the CIO and Cybersecurity Coordinator report to the CTO, who is responsible for high level technology policy, or what CIO Kundra refers to as game changers. It is my intention to address this issue during reauthorization of FISMA, and I look forward to working with the Chairwoman and members of the Subcommittee on this.

As this Subcomittee has learned from multiple hearings on cybersecurity, federal agencies have largely come into compliance with FISMA cybersecurity requirements without actually making our information systems secure from attack. We are training over 90% of our employees but those trainings haven't translated into information security. Fortunately, President Obama is focused on developing performance metrics that could improve agencies' information security, and has established an Office of Personnel Management task force to develop these metrics. We must use the FISMA reauthorization to shift from compliance to performance based measures if we are going to keep pace with the continuing development of advanced cybersecurity threats.

Thank you again for holding this hearing, and I hope to hear from the panelists about this two issues as we prepare to reauthorize FISMA.

Ms. WATSON. Thank you.

We now yield to Mr. Duncan for an opening statement.

Mr. DUNCAN. Well, thank you very much, Madam Chairwoman. Certainly, this is a very important topic. The statistics are almost mind-boggling. In spite of all the money that is being spent on this and all the efforts that are being made, the number of security incidents keeps going up.

Our committee memorandum tells us that there were roughly 90,000 breaches in 2008, and that figure went to the figure that we have in our folder, 108,710, in 2009. It reminded me that several years ago, as I was coming back from lunch in Knoxville 1 day, I heard on the CBS radio national news in my car that the top secret files at the Pentagon had been broken into. It was something approximately 250,000 times that year, or 200,000 times. And that figure was matched a few months ago in this committee when we had the head of a company that said, just to show that they could do it, they downloaded 250,000 individual tax returns.

So, because of all these things, I have begun to wonder if there really is such a thing as cybersecurity, or is it just something for companies to make money off of. I would be very interested in the testimony. Unfortunately, because of previously scheduled appointments, I was only going to be able to be here from 2 until 2:45, and my 2:45 appointment is already here. So I apologize to the witnesses.

But I can assure you that I will read your testimony and your responses to what I have just said with great interest, because I am becoming more and more skeptical. It seems to me that something needs to be done, but are we pouring money down a rat hole? You know, it seems to me that we started out controlling the computers, and now they control us. And I know that all the young people worship their computers, but, this security business, I think people need to realize that anything that they put into a computer is just not secure at all, at least at this point.

Thank you.

Ms. WATSON. Thank you.

Now that we have no further opening statements, 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. Let the record reflect that the witnesses answered in the affirmative.

I will now introduce our panelists.

Mr. Vivek Kundra is 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 technology spending. Prior to joining the Obama administration, Mr. Kundra served in Mayor Fenty's cabinet as the Chief Technological Officer for the District of Columbia and Governor Kaine's cabinet as Assistant Secretary of Commerce and Technology for the Commonwealth of Virginia.

Mr. Gary "Gus" Guissanie is the Acting Deputy Assistant Secretary of Defense for Identity and Information Assurance at the Department of Defense. There, he is charged with implementing DOD programs that require planning, monitoring, coordinating, and integration of information assurance across its component agencies.

Mr. Streufert is the Deputy Chief Information Office for Information Security at the Department of State. He is responsible for providing oversight and guidance for information assurance activities, including security policy development, risk management, systems authorization, training and awareness, compliance reporting, and performance measures. Prior to his tenure at State, he served in various IT management roles at USAID, USDA, and the U.S. Navy.

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, and he is the GAO's leading expert on FISMA implementation.

I would like to ask all of you, and I ask that each of the witnesses now give a brief summary of their testimony, and we would like to have you keep this summary under 5 minutes in duration if you can, because your complete written statement will be included in the hearing record. And I would like to please start with Mr. Kundra.

STATEMENTS OF VIVEK KUNDRA, CHIEF INFORMATION OFFICER, OFFICE OF MANAGEMENT AND BUDGET; GARY "GUS" GUISSANIE, ACTING DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR CYBER, IDENTITY, AND INFORMATION ASSURANCE, U.S. DEPARTMENT OF DEFENSE; JOHN STREUFERT, DEPUTY CHIEF INFORMATION OFFICER FOR INFORMATION SECURITY, BUREAU OF INFORMATION RESOURCES MANAGEMENT, U.S. DEPARTMENT OF STATE; AND GREGORY WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

STATEMENT OF VIVEK KUNDRA

Mr. KUNDRA. Great. Good afternoon, Madam Chairwoman and members of the subcommittee. Thank you for the opportunity to testify on the state of Federal information security and the current challenges we face.

Cybersecurity is a Presidential priority and across the administration we are working on this issue. I work closely with the President's Cybersecurity Coordinator, Howard Schmidt, and the Federal Chief Technology Officer, Aneesh Chopra.

Eight years ago, when FISMA was enacted, the mobile computing revolution and the Internet were not as pervasive as they are today. Agencies are leveraging technologies and business models today that were not present at the time, from cloud computing to mobile platforms. These new models increase efficiency, but also leave agencies struggling with questions on how they apply FISMA's requirements in an environment where boundaries no longer determine security points. Agencies have made significant

progress in complying with FISMA requirements; yet, the Federal Government is still far from secure.

The annual FISMA measures have led agencies to focus on a culture of compliance. However, we cannot get to security through compliance alone. Significant issues have hindered the Federal Government's effectiveness in cybersecurity, including a lack of coordination, a culture focused on compliance, a failure to take an enterprise approach, and a fragmented research and development agenda.

To coordinate the many cybersecurity activities across the Government, the President appointed Howard Schmidt. Mr. Schmidt serves as a key member of the President's national security staff while working in tandem with the private sector on cybersecurity. Additionally, the Department of Homeland Security, in coordination with the White House and various stakeholders from Government and industry, is developing a National Cyber Incident Response Plan. This plan will focus on outlining key roles and responsibilities across the Nation, linking all levels of Government and the private sector.

In 2009, we began shifting agencies to a culture that would focus more on performance and less on compliance. Last October, OMB launched CyberScope, a platform which collects performance metrics enabling meaningful analysis of the agency's security posture. Since metrics are policy statements that influence how agencies deploy resources, OMB established a task force to develop performance-based security metrics.

This work resulted in a three-tiered approach that will be implemented through CyberScope. Data feeds, security posture questions, and making sure that we are specifically focusing on the risks at specific agencies, from Health and Human Services to the Department of Defense to the State Department, which have very different missions and risk profiles. This approach will provide essential information about agency security postures, activities, and threats.

We should also drive agencies toward continuous monitoring of security-related information across their organizations. It is necessary to take an enterprise approach to cybersecurity. That is why we are leveraging governmentwide vehicles to enable agencies to purchase security tools efficiently. To energize the Nation's research and development efforts, the administration is encouraging innovation in game-changing technologies to shift the advantage from the attacker to the defender. These activities include efforts such as National Cyber Leap Year and the National Research and Development Summit we just did, the creation of a group designed to look at the financial services sector and create a test bed where we could model scenarios that we need to defend against and also the establishment of an industry, academia, and government working group to explore cybersecurity insurance as a market force to improve security across the board.

Security is a journey, not a destination. We are moving forward. For example, the Government has won praise for their work done to contained Conficker. A representative of the Conficker Working Group, an independent group of private sector companies focused on defeating the Conficker worm said, "For the first time the gov-

ernment is taking the lead in a technical security issue, rather than lagging."

This is where we want to be. Unfortunately, the State Department spent $133 million over the last 6 years on paperwork compliance. But under the leadership of John they have made significant changes to how they approach this problem. But what we really need to do is not file paperwork in metal cabinets. Instead, we should shift to constantly testing for weaknesses. That is why the President's 2011 budget provides funding for red teams and blue teams to conduct penetration testing on Federal systems.

A secure trusted computing environment in the Federal Government is the responsibility of everyone involved; agency heads, the Federal work force, and contractors who support us. This will not be easy, nor will it take place overnight. Together with the Cybersecurity Coordinator, Howard Schmidt, and the Chief Technology Officer, Aneesh Chopra, we will continue to address challenges that face our Nation in cyberspace.

Thank you for the opportunity to testify. I look forward to your questions.

[The prepared statement of Mr. Kundra follows:]

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

March 24, 2010

STATEMENT OF VIVEK KUNDRA
FEDERAL CHIEF INFORMATION OFFICER,
ADMINISTRATOR FOR E-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

"Federal Information Security: Current Challenges and Future Policy Considerations"

Good morning, Madam Chairwoman and members of the Subcommittee. Thank you for the opportunity to testify on the state of Federal information security and the current challenges and future policy considerations.

The globally interconnected digital information and communications infrastructure known as "cyberspace" underpins almost every facet of modern society and provides critical support for the economy, civil infrastructure, public safety, and national security. To realize the full benefits of the digital revolution, the American people must have confidence that sensitive information is not compromised, their communications with the government are secure, their privacy and civil liberties are protected, and that the Federal infrastructure is not infiltrated. Achieving trusted communications and information infrastructure will ensure that the United States achieves the full potential of the information technology revolution.

The group of actors who target U.S. citizens, businesses, and Federal agencies is growing. US-CERT, the computer readiness center for civilian agencies, sees millions of attempts daily to access open ports and vulnerable applications on Federal networks.

Cybersecurity is a Presidential priority and, across the Administration, we are working on this issue. I am working closely with the President's Cybersecurity Coordinator, Howard Schmidt, and the Federal Chief Technology Officer, Aneesh Chopra. As Cybersecurity Coordinator, working as part of both the National Security Staff and the National Economic Council, Mr. Schmidt is coordinating cybersecurity activities across the government, including those under the Comprehensive National Cybersecurity Initiative (CNCI). As the Federal Chief Technology Officer, Aneesh Chopra is focused on advanced, "game-changing" technologies that help the government meet not only the threats of today, but those of the future as well. As the Federal Chief Information Officer, I am charged with OMB's responsibilities under the Federal Information Security Management Act (FISMA).

Eight years ago, when FISMA was enacted, the internet and the mobile computing revolution were not as pervasive as they are now. Today, agencies are leveraging technologies and business models such as cloud computing, mobile platforms, social media, and third-party platforms to increase efficiency and effectiveness. For example, the Department of Veterans Affairs contracts with mortgage services to service VA-owned home loans. These new models increase efficiency but leave agencies struggling with the question of how to apply FISMA's requirements in an environment where system and enterprise boundaries no longer define the security points. Effective cybersecurity is vital to our national prosperity and economic stability; however, cyber incidents continue to impact the Federal Government.

2009 FISMA REPORT SUMMARY

In the past eight years, agencies have made significant progress in complying with FISMA requirements. For example in Fiscal Year 2002, 35% of agency systems had tested contingency plans; whereas, by the end of Fiscal

Year 2009, 86% of agency systems had tested contingency plans. In 2002, 60% of agency systems had tested security controls; whereas, in 2009, 90% agency systems had tested security controls.

Agencies have also reported improvements in their compliance with Certification and Accreditation (C&A) requirements such as assessing their systems for risks and creating system security plans. In 2002, 47% of all agency systems had a Certification & Accreditation in place; whereas, in 2009, 95% of systems had a Certification & Accreditation in place.

Similarly, agencies reported substantial progress in the training of employees with significant security responsibilities, increasing the skills of the Federal cybersecurity workforce. In 2002, 37% of employees with significant security responsibilities were trained; whereas in 2009, 90% were trained.

Agencies also provided details on headcount and training costs in their FY 2009 FISMA reports. In FY 2009, agencies reported 64,450 FTEs dedicated to cybersecurity; however, 90% of those FTEs reported reside within the Department of Defense. Of the $6.8 billion in total cybersecurity spending reported by agencies in the FY 2009 budget, $54.6 million (less than 1%) was spent on training. This amount includes the annual security awareness required for all Federal employees and contractors, as well as training for employees with significant cybersecurity responsibilities.

Despite the improvements as reported by agencies, the Federal Government's communications and information infrastructure is still far from secure. The FISMA measures reported on annually have led agencies to focus on compliance. However, we will never get to security through compliance alone.

KEY ISSUES IN FEDERAL CYBERSECURITY

President Obama has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity." As a result, in February 2009, the President directed the National Security Council and Homeland Security Council to conduct a review of the plans, programs, and activities underway throughout government that address our communications and information infrastructure (i.e., "cyberspace"), in order to develop a strategic framework to ensure that the U.S. Government's initiatives in this area are appropriately integrated, resourced, and coordinated.

There are a number of issues that contribute to our vulnerabilities, including:

I. **Lack of Coordination** – There has been no single individual or entity with the responsibility to coordinate Federal Government cybersecurity-related activities, both within the Federal Government and with the private sector. Many departments and agencies have disparate responsibilities with regards to cybersecurity. Furthermore, even for specific cyberthreats and incidents, agency responses are often fragmented and uncoordinated with each other. Independent efforts are not sufficient to address the challenges without a central coordination mechanism, an updated national strategy, an action plan developed and coordinated across the Executive Branch, and the support of Congress.

II. **Culture of Compliance** – For too long, Federal agencies have focused on reporting on security rather than gaining meaningful insight into their security postures. For example, over the last six years, the Department of State spent $133 million amassing a total of 50 shelf feet, or 95 thousand pages, of security documentation for about 150 major IT systems. This works out to roughly $1,400 per page on paper "snapshots" that are often outdated a few days after being published.

III. **Lack of an Enterprise Approach** – Currently, security information is scattered throughout agencies in different systems that do not communicate with each other. For example, in previous security incidents, some agencies had difficulty determining how many of their computers were vulnerable, how many were patched, and how many were infected across their enterprises. Similarly, defense of Federal networks is fragmented and lacking clear situational awareness.

IV. **Energize National Agenda for Cybersecurity Research & Development** – The United States needs to harness the full benefits of innovation to address cybersecurity concerns. Currently, multiple agencies have cybersecurity R&D activities on-going. The challenge is to focus these activities to achieve the most significant advances and to give the Federal Government and the public stronger cybersecurity.

ADVANCING THE SECURITY POSTURE OF THE FEDERAL GOVERNMENT

To advance the security posture of the Federal Government, the Administration is taking a number of actions, including focusing on coordination, shifting to a performance-based culture, taking an enterprise approach to cybersecurity, and developing an integrated plan for research and development.

I. Focusing on Coordination

To address the lack of coordination, the Administration has taken the following steps.

Cybersecurity Coordinator – On December 22, 2009, the President appointed Howard Schmidt as his Cybersecurity Coordinator. Mr. Schmidt has the responsibility of orchestrating the many important cybersecurity activities across the government; in particular, those related to the Comprehensive National Cybersecurity Initiative (CNCI), and serves as a key member of the President's National Security Staff. Mr. Schmidt oversees Federal-wide coordination of the President's cybersecurity agenda, while working in tandem with the private sector on cybersecurity.

Coordination in cybersecurity research and development is discussed below in section IV.

II. Shifting to a Performance-Based Culture

For too long, the focus in Federal security has been on compliance rather than performance. In 2009, we began moving agencies to a performance-based culture.

Declassified Description of the Comprehensive National Cybersecurity Initiative – The CNCI constitutes an essential component of cybersecurity efforts within the Federal Government. On his first full day in office, in a memorandum on open government to all Federal departments and agencies, President Obama said, "My Administration is committed to creating an unprecedented level of openness in government." Building on this statement, on March 2, 2009, the Administration revised the 2008 classification guidance for the CNCI. An unclassified description of the CNCI and each of the 12 initiatives under the CNCI is now publicly available.

Transparency is particularly vital in areas such as the CNCI where there have been legitimate questions about sensitive topics like the role of the intelligence community in cybersecurity. Transparency provides the American people with the ability to partner with government and participate meaningfully in the discussion about how we can use the extraordinary resources and expertise of the intelligence community with proper oversight for the protection of privacy and civil liberties.

Launch of CyberScope – On October 19, 2009, OMB launched an interactive data collection tool—CyberScope—enabling agencies to fulfill their FISMA reporting requirements through a modern digital platform. The broad range of information collected, the use of secure two-factor authentication using Personal Identity Verification (PIV) cards, and the online access to data provide for a more efficient and effective reporting process , allow for the collection of more complex metrics and enable more meaningful analysis of agency security postures. CyberScope empowers its 600 estimated users to manage their internal reporting and information collection processes as best suits their individual needs, while allowing OMB better access to agency security information.

Performance-Based Metrics – In September 2009, OMB established a task force to develop new, outcome-focused metrics for information security performance for Federal agencies. To solicit the best ideas, OMB reached out across the Federal community as well as to the private sector. This task force concentrated on developing metrics that would advance the security posture of agencies and departments.

Understanding that metrics are a policy statement about what Federal entities should concentrate resources on, the task force developed metrics that will push agencies to examine their risks and make substantial improvements in their security. Participants in the task force included: the Federal CIO Council; the Council of Inspectors General on Integrity and Efficiency; NIST; the Department of Homeland Security; the Information Security and Privacy Advisory Board; and the National Security Council Cybersecurity Coordinator. In addition, the Government Accountability Office (GAO) served as an observer to this taskforce.

The result of the work done by the taskforce is a three-tiered approach for FY 2010 FISMA reporting for agencies through CyberScope: data feeds; security posture questions; and agency interviews.

Continuous Monitoring – The key element to managing an information security program is information—about agencies' security postures, activities and threats. Agencies need to be able to continuously monitor security-related information from across the enterprise in a manageable and actionable way. The many levels of agency management all need different levels of this information presented to them in ways that enable timely decision making.

A critical aspect for agency officials of managing risk to information from the operation and use of information systems involves the continuous monitoring of the security controls employed within or inherited by the system. Conducting a thorough point-in-time assessment of the deployed security controls is a necessary but not sufficient condition to demonstrate security due diligence. An effective organizational information security program also includes a rigorous continuous monitoring program integrated into the system development life cycle. A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to organizational officials in order to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of the information system.

Collection of Information Security Costs – In this reporting cycle, for the first time, OMB asked agencies for detailed cost estimates and the actual amounts spent on information security. Historically, as part of the annual budget process, agencies reported only the percentage of spending related to cybersecurity for each IT investment. However, this information was not broken down into distinct categories, such as personnel costs, reporting costs, certification and accreditation (C&A) costs, and security management costs. This lack of detailed information precluded the level of meaningful analysis needed to assess the efficiency and effectiveness of Federal information security spending.

Recognizing that the best security is "baked in" to information technology investments and not added in separately or well after the investments have been deployed, OMB needs to determine where, in the life cycle development of systems, agencies are spending their resources. The information collected for FY 2009 is the beginning of the process of obtaining this crucial cost data.

In the coming years, access to continually refined cost data will allow OMB to evaluate the efficiency of Federal expenditures on security. The collection of detailed information, especially when combined with performance-based metrics, will allow both OMB and agency management to make informed, risk-based decisions on where to allocate scarce resources.

TechStat – In June 2009, we launched the IT Dashboard, which allows the American people to monitor IT investments across the Federal Government. Building on the foundation of the dashboard, we launched TechStat Accountability Sessions this past January. A TechStat accountability session is a face-to-face, evidence-based review of an IT program with OMB and agency leadership, powered by the IT Dashboard and input from the American people. TechStat sessions enable the government to turnaround, halt or terminate IT investments that do not produce dividends for the American people. Investments are carefully analyzed with a focus on problem solving that leads to concrete action to improve performance. In particular, we have applied this approach to Federal IT security projects. For instance, several of the TechStats conducted to date have focused on security such as agency HSPD-12 implementation efforts.

III. Enterprise Approach to Cybersecurity

To achieve true situational awareness and to fully harness the power of the Federal Government to address the challenges of cybersecurity, we must take an enterprise approach. We are taking a number of steps to move us forward, including:

Improve the Effectiveness of the Cybersecurity Workforce – The White House has formed an interagency working group to establish the National Cybersecurity Education Initiative. This working group defined four tracks of work that are now underway:

- Track 1 – A National Awareness Campaign led by the Department of Homeland Security;
- Track 2- A Formal Cybersecurity Education program led by the Department of Education;
- Track 3 – A Federal Workforce Structure program led by the Office of Personnel Management and the Department of Defense; and
- Track 4 – A National Workforce Training and Professional Development Program led by the Departments of Homeland Security and Defense, and the Office of the Director of National Intelligence.

Achieve a Consistent Security Posture – Through initiatives such as the Trusted Internet Connections (TIC) initiative and the Federal Desktop Core Configuration (FDCC), we are standardizing good security practices across the Federal enterprise. The TIC initiative is composed of two distinct efforts. The first is to reduce the target profile of Federal agencies by decreasing the number of external access points. The second is to implement an Intrusion Detection System using passive sensors to identify when unauthorized users attempt to gain access to those networks.

The FDCC establishes a consistent security configuration for desktops and laptops running Windows-based software across Federal agencies. This configuration includes basic security measures such as turning off ActiveX controls, a common infection vector, by default.

Coordinate Incident Response – The President's Cyberspace Policy Review identified response and coordination efforts around cyber incidents as a key area for improvement. As a result, the Department of Homeland Security, in coordination with the White House and various stakeholders from government and industry, is developing a new National Cyber Incident Response Plan (NCIRP). The NCIRP will outline key cyber roles and responsibilities across the Nation, linking all levels of government and the private sector. It is intended to describe how every day, steady-state cyber incident management activities expand to manage incidents that require a coordinated National response.

Leverage Federal Purchasing Power – We are leveraging Blanket Purchase Agreements (BPAs) and other government-wide acquisition vehicles to enable agencies to purchase security tools in an efficient manner. For instance, in Q4 2009, a BPA was announced that included tools to help agencies develop an accurate inventory of information resources managed at their agency, and maintain an up-to-date awareness of information regarding cybersecurity threats.

Implement Federal Identity Management – The ability of Federal agencies to accept credentials of other agencies' employees is fundamental to government-wide coordination. As part of this effort, OMB continues to oversee the implementation of the strong Federal identity management scheme outlined in Homeland Security Presidential Directive 12 (HSPD-12) ("Policy for a Common Identification Standard for Federal Employees and Contractors") which requires agencies to follow specific standards and business processes for the issuance and use of Personal Identity Verification (PIV) smartcard credentials. When used in accordance with NIST guidelines, the credentials provide a number of benefits including secure access to Federal facilities and disaster response sites, as well as multi-factor authentication, digital signature and encryption capabilities. As of December 1, 2009, over 5 million PIV credentials (82 percent of those needed) had been issued to the Federal workforce, as reported by agencies.

Moving beyond Federal identity management, the Cyberspace Policy Review also calls for development of a "cybersecurity focused identity management vision and strategy." In response to this requirement the White House has established an effort to develop a National Strategy for Secure Online Transactions. The goal of this effort is to improve the trustworthiness and security of online transactions by facilitating the establishment of interoperable trust frameworks and implementation of improved authentication and authorization technology and processes for all online transaction participants, across Federal, civil, and private sectors. OMB, in conjunction with the Federal CIO Council, has developed PIV-interoperability policy and criteria for acceptance of non-Federal credentials.

IV. Develop an Integrated Plan for Research & Development

The President's Cyberspace Policy Review calls for sharing responsibility for cybersecurity by improving the partnership between the private sector and government; and encouraging innovation in game-changing technologies in coordination with industry and academia. This expands on the goal of the Comprehensive National Cybersecurity Initiative (CNCI) to strengthen the future cybersecurity environment by coordinating and redirecting research and development efforts across the Federal Government.

These goals have been embraced under White House leadership. Progress includes (1) The National Cyber Leap Year, gathering input from more than 300 private sector white papers and a National Summit to develop a shared game-changing R&D strategy focused on moving target, tailored trustworthy spaces, and cyber economic incentives; (2) a joint Financial Services Sector/government task group, developing a real-traffic cybersecurity testbed; and (3) a working group of industry leaders, university researchers, and government representatives formed around cybersecurity insurance as a market force for improved security.

The Cybersecurity and Information Assurance (CSIA) Interagency Working Group coordinates R&D activities for unclassified efforts, the Special Cyber Operations Research and Engineering (SCORE) group for classified activities, and the Senior Steering Group for Cybersecurity (SSG) bridges these groups and provides overall direction and guidance. Research supported under these efforts and conducted in both government and private settings includes cybersecurity metrics, security automation, network protection and defense, secure software engineering, and other areas to create the next generation of cybersecurity capabilities.

CLOSING

The Administration has taken a number of steps to improve cybersecurity across the Federal Government in the past year. However, security is a journey, not a destination. The threats we face are numerous, evolving faster than our cyber defense, and have the potential to do great harm. We are moving forward. For example, the Government has won praise for the work we did to contain Conficker. A representative of the Conficker Working Group said, "For the first time the government is taking the lead in a technical security issue, rather than lagging."[1]

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 while respecting the privacy and civil liberties of the American people. This will not be easy nor will it take place overnight. Our current actions represent important steps towards a stronger Federal cyber defense, but we must remain ever-vigilant. I look forward to continuing to confront the challenges our Nation faces in cyberspace in concert with Cybersecurity Coordinator Schmidt and Chief Technology Officer Chopra.

I thank the Committee for this opportunity to appear here today and I look forward to not only answering any questions that you might have but also to working in partnership with you on these critical issues for our government and our nation.

---

[1] Government Computer News, "Have Agencies Scrubbed the Conficker Work From Their Systems?', March 19, 2010, http://gcn.com/articles/2010/03/19/conficker-cleanup-031910.aspx

Ms. WATSON. Thank you, Mr. Kundra.
Now, Mr. Guissanie, you may proceed.

STATEMENT OF GARY "GUS" GUISSANIE

Mr. GUISSANIE. Good afternoon, Chairwoman Watson, Congressman Bilbray, and members of the Government Management, Organization, and Procurement Subcommittee. My name is Gus Guissanie, and I represent the Office of the Assistant Secretary of Defense for Networks and Information Integration and the Department of Defense Chief Information Officer. I want to thank you for the opportunity to appear before the subcommittee to discuss issues related to governmentwide information security, the Department's efforts to comply with FISMA mandates, and initiatives to enhance the Nation's cybersecurity.

Cybersecurity is and has been a critical priority for the Department of Defense. Our information systems, which are globally distributed and connected to coalition and interagency partners, are essential to our DOD missions; therefore, we must have a robust, assured enterprise network.

In concert with the administration's Government-wide information security objectives, we support a focus on continuous monitoring and the use of real-world penetration testing to ensure a robust security posture. However, the DOD policy of conducting stringent security testing prior to an authorization to operate remains a critical element of information assurance.

The Department has found FISMA in its current form to have significant strengths in improving cybersecurity, and would point out that any deficiencies in implementations are not, in and of themselves, sufficient justification for major change or reform.

One construct that the Department believes is valuable in the current statute and should be retained is the organizational relationship between the Agency Chief Information Officer [CISO], and the Agency CIO. A CISO cannot effective function if separated organizationally from the CIO and the operational activity being protected.

I would now like to highlight some DOD initiatives taken to secure our systems within the framework of current FISMA legislation.

The Department has been working to develop information assurance metrics at the strategic and operational levels both within the Department and the broader Federal community. As we seek metrics which provide our leadership decisionmaking insight, we are working toward the capability to accomplish risk scoring in prioritized vulnerability remediation based on actual threat activity to enable a more active and flexible defense.

The Department is also implement a series of initiatives aligned to our DOD information assurance strategy with several accelerated in fiscal year 2009 by the Comprehensive National Cybersecurity Initiative. For example, we are deploying a host-based security solution for continuous monitoring and protection against threats. We are hardening our unclassified network by improving censoring, filtering, and access control at our Internet access points or gateways, thus limiting exposure of critical information. By changing our access control technologies and methodolo-

gies to ensure that only our public-facing servers are accessible from the Internet, we have reduced this attack surface by 96 percent.

We have expanded cooperation with hour defense industrial base to protect unclassified defense-related research, development, and procurement information, and we are also working with the Department of Homeland Security to develop a multi-pronged approach for managing supply chain risks arising from the globalization of the information and communications technology marketplace.

A skilled cyber work force is the most critical component of our defense against cyber adversaries. Therefore, the Department is continuing to raise the bar through our Workforce Improvement Program, extend our IA range capability, and ensure quality training is available to our work force. Additionally, the 106 National Centers of Academic Excellence in IA Education are producing graduates with the right skills to become a world-class cyber work force.

I would like to conclude by emphasizing that we continue to work toward a resilient and dependable enterprise network for the Department and the Nation. We are accomplishing this through collaboration with other Federal agencies to resolve security issues impacting Government-wide shared services and infrastructure. The DOD CIO is managing a diverse portfolio to enable worldwide operations supporting over 2½ million users that is aggressively working to get ahead of the daunting global security challenge.

I am happy to take your questions.

[The prepared statement of Mr. Guissanie follows:]

STATEMENT BY

MR. GARY GUISSANIE

ACTING DEPUTY ASSISTANT SECRETARY OF DEFENSE

FOR IDENTITY AND INFORMATION ASSURANCE

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

SUBCOMMITTEE ON

GOVERNMENT MANAGEMENT, ORGANIZATION AND PROCUREMENT

2154 RAYBURN HOUSE OFFICE BUILDING
MARCH 24, 2010
2:00 P.M.

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT
ORGANIZATION AND PROCUREMENT

Good afternoon, Chairwoman Watson, Congressman Bilbray, and Members of the Government Management, Organization and Procurement Subcommittee. I am Gary "Gus" Guissanie representing the Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (CIO). I want to thank you for the opportunity to appear before the Subcommittee to discuss issues related to government wide information security, the Department's efforts to comply with existing FISMA mandates, and initiatives to enhance the nation's cybersecurity[1] through FISMA reform as we go forward.

To paraphrase the Secretary's February 2, 2010, House Armed Services Committee testimony, our military forces depend on digital communications and the satellites and data networks that support them. We face adversaries from individual hackers to nation-states that may seek, without attribution, to damage our command and control operations, intelligence, surveillance, reconnaissance, or precision strike capabilities. With relatively accessible technology and minimal investment, our adversaries operating in cyberspace may, without attribution, damage our command and control operations; intelligence, surveillance, reconnaissance or precision strike capabilities.

[1] The U.S. Government currently defines *cybersecurity* as "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation." (NSPD 54/HSPD 23).

Cybersecurity is and has been a critical priority for the Department of Defense (DoD). With information and information technology (IT) assets globally distributed and connected to our partners who actively participate in DoD missions, we know that we cannot execute operations without a robust, assured enterprise network.

This enterprise network approach, coupled with skilled users, defenders, and first-responders working collaboratively with our diverse domestic and international government, intelligence, and civilian partners, including the Defense Industrial Base, will enable us to more readily identify and respond to a cyber attack – and fulfill our missions.

As has been discussed previously before this Subcommittee, the DoD cybersecurity program is aimed at ensuring the following vision:

- DoD missions and operations continue under any cyber situation or condition.
- The cyber components of DoD weapons systems and other defense platforms perform as expected.
- The Department has ready access to its information, including command and control systems, and its adversaries do not.
- The Defense information environment securely and seamlessly extends to mission partners.

Within the Department's overall cybersecurity strategy, a key goal is to "anticipate and prevent successful attacks on data and networks," which closely aligns with the issues being discussed in the community regarding how to better implement cybersecurity measures to defend against increasing cyber threats and vulnerabilities. In concert with the Administration's government-wide information security objectives, we support the focus on continuous monitoring and on the use of real-world penetration testing to maintain a robust security posture. We also consider DoD policies of stringent security testing prior to authorization of systems operation to be a critical element of information assurance. Today, we are progressing toward an enterprise information environment that can dynamically and automatically configure itself to counter threats and facilitate our missions.

FISMA Legislation

The Department has found FISMA in its current form to have significant strengths in improving cybersecurity and would point out that any deficiencies in implementations are not, in and of themselves, sufficient justifications for reform.

One construct that the Department believes is valuable in the current statute that should be retained is the current organizational structure and relationship between the Agency Chief Information Security Officer (CISO) and the Agency CIO. A CISO cannot function effectively if separated organizationally from the CIO and from the operational activity being protected.

DoD Information Assurance Efforts

I will now address Department initiatives to secure our systems within the framework of current FISMA legislation:

DoD Implementation of FISMA

The Department is playing a significant role in multiple efforts to improve the implementation of FISMA. One of those efforts is improving performance metrics and in particular metrics which are feasible for large agencies such as the DoD. The Department recommended a number of improvements to the proposed performance metrics, including:

- Identification of metrics, at the appropriate level of detail, that provide useful information to leadership for assessing the security posture of the organization and enterprise.
- Focusing the proposed automated collection of metrics on the most important metrics for security and management oversight. The Department has been working IA metrics at both strategic and operational levels. As we consider which metrics provide valuable leadership decision-making insight, we are working toward a capability to accomplish "risk scoring" in order to prioritize vulnerability remediation. Eventually we intend to include information on actual threat activities, along with vulnerability data, to enable a more active and flexible defense. Initiatives that roll up raw data, for example: counting workstations, servers, and their operating system versions, when averaged into compliance percentages, lose their meaning when out of

the context of their operational environment. This is particularly true across an environment the size of DoD, or the Military Departments, Defense Agencies or other Defense Components. Because of this, we are building metrics to provide a strategic understanding to senior leadership while employing metrics for the operational Commands.

DoD CNCI and Other IA Activities

The Department is actively implementing a series of initiatives in concert with its IA Strategy and support for the Comprehensive National Cybersecurity Initiative (CNCI). While the Department is aggressively enhancing the security of our systems and networks, the cyber threats in an information-centric world are significant and increasing. Conducting counterterrorism operations, global peacekeeping, homeland security and preparing for escalated warfare make it imperative that IA be viewed not as an IT expense, but as a critical enabler of all national security and defense capabilities. As part of the CNCI and our overall IA Program, the Department is supporting a number of important initiatives, including:

- Acquiring and deploying innovative technologies such as the Host Based Security Solution (HBSS) to increase the fundamental end-point security of our cyber enterprise; thus setting the stage for a unified security baseline. This automated solution will improve security management while reducing costs; increasing the networks' survivability and recovery; and allowing for rapid response to threats targeting the Department.

- NIPRNet Hardening: DoD realigned its access control methodology and operations at the Nonclassified Internet Protocol Router Network (NIPRNet) Internet Access Points, moving from a permit all, deny access by exception policy, to blocking unauthorized access to our private information and supporting systems through whitelisting. Whitelist access is now being used to ensure that only our public facing servers are accessible from the Internet, ensuring that our private servers are not accessible. The most immediate result of these efforts has been to reduce our attack surface by 96 percent. With the full implementation of perimeter DMZs, we will be able to isolate/filter malware at the Internet boundary. As an example, with the removal of spam and malware (viruses, etc.), our first customers at the initial email security gateways have had their traffic loads reduced by 90 percent.
- Defense Industrial Base (DIB): Established a pilot cybersecurity program for the Defense Industrial Base to protect unclassified information relevant to Defense-related research, development and procurement. This effort provides the mechanism to exchange relevant threat information in a timely manner, provides intelligence and digital forensic analysis on threats, and expands Government to Industry cooperation while ensuring that industry equities and privacy are protected. To further this effort, an Advanced Notice of Public Rulemaking was recently published on a possible change to the Defense Federal Acquisition Regulation Supplement (DFARS), which will codify implementation of these pilot security capabilities with our industry partners.

- Supply Chain Risk Management (SCRM): DoD is a co-lead with DHS working to develop a multi-pronged approach for managing risks arising from the globalization of the information and communications technology marketplace. DoD issued a Supply Chain Risk Management Policy now being implemented through several pilot efforts, and the Defense Intelligence Agency has established a Threat Analysis Center to provide supply chain threat assessments to the DoD acquisition community. In January of this year, DoD delivered its "Trusted Defense Systems" report to Congress as we implement a comprehensive trusted defense system strategy targeting full operating capability by fiscal year 2016.
- Joined forces with other federal agencies in the CNCI to secure government networks, protect against constant intrusion attempts, and anticipate future threats.
- Developed and updated the DoD Cyber, Identity and Information Assurance (CIIA) Strategic Plan.
- Partnered with the DNI to establish the Unified Cross Domain Management Office (UCDMO) to synchronize and accelerate the availability of all levels of classified/sensitive information and to protect sensitive or controlled unclassified information to include sharing with our closest partners.
- Contributing DoD expertise to address government-wide information security concerns by partnering with other Federal CIO's and CISO's. The Department is supporting this effort through, among other means, the Department of the Navy CIO co-chairing the Federal CIO Council's Information Security and Identity Management Committee (ISIMC).

- Teamed with the Department of Commerce, the Office of the DNI, and the Committee on National Security Systems (CNSS) to produce a unified information security framework for the federal government -- including a consistent process for selecting and specifying safeguards and countermeasures (i.e. security controls) for federal information systems. This group has already revised control sets for federal civilian and NSS in fiscal year 2009 and, in February of this year, issued the innovative process of the Risk Management Framework as a replacement of the security certification and accreditation (C&A) process.
- Developed Department-wide information systems C&A reciprocity procedures that will ensure the rapid and secure fielding of DoD information systems. Reciprocity will allow mutual agreement among participating enterprises to accept each other's security assessments in order to reuse Information System resources and to accept each other's assessed security posture in order to share information.
- Integrating network and cyber operations in conjunction with the United States Strategic Command to increase our ability to defend the DoD systems and networks.
- Accredited 25 Computer Network Defense Service Providers (CNDSPs) or "CERTS" across DoD.
- Partnered with the National Counterintelligence Executive and Insider Threat Advisory Group to foster collaboration on the use of insider threat tools.
- Promulgated policy on effective use of Internet-based capabilities, including social networking services within the DoD.
- Participating in government-wide cloud computing efforts and a working group

addressing NIST controls for cloud computing.

- DoD also provides a Shared Service Center for Federal IA awareness training at no cost to the participating Federal Agencies.
- Continued to expand the scope and quality of cyber training available to the Department's workforce. In addressing heightened concerns over civil liberties and identity theft, this training includes a review of privacy safeguards and responsibilities to protect personally identifiable information.
- Provided the foundation for the Federal Desktop Core Configuration (FDCC) for a government-wide security baseline for the Windows XP and Vista Operating Systems (OS's). We are continuing our leadership role in this initiative through NSA releasing the draft Windows 7 configuration in fiscal year 2010 and ongoing efforts on other OS's.

DoD IA Workforce

The Department places significant focus on our cyber workforce to help defend the systems and networks. While we aim to achieve robust machine-to-machine network defense capabilities, skilled experts will always remain a critical component in our defense against cyber adversaries. From the everyday user to the cyber defender, the DoD workforce needs to be fully trained and qualified, appropriately deployed, and effectively manned to leverage and protect the Department's significant investment in information and communications. Competency in multiple cybersecurity skills is

demonstrated and evaluated throughout the cybersecurity community through the conduct of joint exercises and is an ongoing core priority of the Department.

To this end, the Department is continuing to expand the IA range capability and quality of cyber training available to its workforce. The technical schools of the military services have expanded their information assurance/cybersecurity curricula to meet DoD common baseline training and certification requirements. The Department has also developed IA awareness training to help users and leaders to better understand their roles in defending DoD networks. In addition, the national Centers of Academic Excellence (CAE) in IA Education are producing graduates with the right skills to achieve a world class cyber workforce that includes both defensive and offensive capabilities. Currently, there are 106 CAEs in 37 states, the District of Columbia, and Puerto Rico, and 32 CAE IA Research Centers in 25 states and the District of Columbia.

Summary

In conclusion, the Department has a strong cyber vision, strategy and supporting program. We continue to work toward a resilient and defendable defense-enterprise network for the Department and for the nation, through collaboration with other Federal agencies to resolve security issues impacting government-wide shared services and infrastructures. The ASD(NII)/DoD CIO is managing a diverse portfolio to comply with FISMA while leading the Department toward Net Centric operations and aggressively working to get ahead of the daunting security challenges facing the Department.

Ms. WATSON. Thank you.
Now, Mr. Streufert, you may proceed.

STATEMENT OF JOHN STREUFERT

Mr. STREUFERT. Good afternoon, Chairwoman Watson, Ranking Member Bilbray, and distinguished members of the subcommittee. I am pleased to have this opportunity to testify before the subcommittee regarding the Department of State's capabilities for securing its global information and technology infrastructure. The Department serves as the diplomatic front line in over 270 overseas posts by serving its 70,000 users with the worldwide network and mission-essential software applications.

The foreign policy mission makes an inviting target for attack by highly skilled cyber adversaries. However, the Department's layered approach to risk management allows multiple levels of protection. This protection is accomplished by implementing a matrix of technical, operational, and management security controls designed to thwart network threats, detect, and mitigate vulnerabilities, and strengthen business operations.

In my role as the Chief Information Security Officer, I have become familiar with the benefits, shortcomings, and promising opportunities to buildupon the current Federal Information Security Management Act of 2002. Our goal is to ensure system security for diplomacy while continuously improving the return on investment for each dollar spent on cybersecurity.

The passage of the FISMA Act in 2002 served as a game-changing event for the Federal agency community. FISMA applies to all information used by or on behalf of the Federal department or agency. In this respect, the establishment of a holistic information security program and the responsibility of accounting to oversight entities, including Congress, served as a valuable check in determining the health of an agency's information security program.

The Federal cybersecurity landscape has changed over the past 5 years. The implementation of a Federal cybersecurity program has typically been implemented in past years through manual processes and compliance checks which have competed with the need to implement Web 2.0 technologies in a secure manner, just to name one among many. Meanwhile, our cyber problems have dramatically escalated in severity and frequency. Since 2008, the number of security-related trouble tickets opened in our organization has more than doubled, while malicious code attacks has increased by 47 percent.

In October 2009, OMB launched CyberScope, a secure data collection platform for reporting and formed an interagency task force charged with developing metrics for information security. Important to our efforts, the National Institute of Standards introduced Special Publication 800–37 and an update to increase the emphasis on continuous monitoring. Of special note, the Department of State began supplementing FISMA compliance reports and studies with a risk scoring program scanning every computer and server connected to its network not less than every 36 hours on eight factors and twice a month for safe configurations of software.

The Risk Scoring Program utilizes best practices such as the Consensus Audit Guidelines, which we have mapped against the

way the Department is being attacked. The Department utilizes the Common Vulnerability Scoring System from NIST where scanning tools tag specific risks with point values between 0 and 10, with 10 being the highest vulnerability. When the problem is resolved, risk points are deducted. To this point, the State Department Risk Scoring Program has implemented a subset of the Consensus Audit Guideline controls that are adaptable to automated verification.

In the first year of site scoring ending July 2009, overall risk on the Department's key unclassified network measured by the Risk Scoring Program was reduced by nearly 90 percent in overseas sites and 89 percent in domestic sites. Scores have been relatively stable since then. Notwithstanding this reduction to date, the Department has decided to make it three times more difficult to achieve the same letter grades as part of an ongoing commitment to continuous improvement of this kind in the future.

These methods, however limited, have allowed one critical piece of the Department's information security program to move from snapshot in time previously available under FISMA to a program that scans for weaknesses on servers and personal computers continuously, identifies weak configurations each 15 days, issues letter grades monthly to senior managers tracking the progress for their organization in closing against known vulnerabilities the last 30 days. It is the Department's objective to expand automated verification to as many Consensus Audit Guideline control categories as possible, to all infrastructure and applications as soon as possible, limited only by available resources.

In short, the details of this program empower administrators of our systems with targeted daily attention to conduct remediation and the summaries empower executives to oversee the most serious problems.

The balance of my statement references additional layers of control, including a 24/7 network watch program, close coordination with incident management at US-CERT; implementation of EINSTEIN 2 for situational awareness; important emphasis on Cyber Threat Analysis which we share with other members of the foreign affairs community; a Global Security Scanning program, a Cybersecurity Incident Program to assure that our employees do not commit acts of cyber misuse or abuse; an awareness training program that we conduct not only for ourselves, but for other members of the Federal Government under the information security line of business.

I want to conclude by emphasizing the Department's policy, technology, business processes, and partnerships in place continue to evolve and meet the ongoing challenges of security threats in the cyber environment.

I would like to thank the subcommittee members for this opportunity to speak before you today, and I would be pleased to respond to any of your questions.

[The prepared statement of Mr. Streufert follows:]

Statement of
John Streufert
Chief Information Security Officer /
Deputy Chief Information Officer for Information Security
Bureau of Information Resource Management
United States Department of State

Before the
House Committee on Oversight and Government Reform
Subcommittee on Government Management, Organization, and Procurement

Federal Information Security: Current Challenges and Future Policy Considerations

2154 Rayburn House Office Building
March 24, 2010
2:00 p.m.

Good afternoon Chairwoman Watson, Ranking Member Bilbray, and distinguished Members of the Subcommittee:

I am pleased to have this opportunity to testify before the Subcommittee regarding the Department of State's capabilities for securing the Department's global information and technology infrastructure. The Department serves as the "diplomatic front-line" in over 270 overseas posts by serving its 70,000 users with a world-wide network and mission essential software applications. The foreign policy mission makes an inviting target for attack by highly skilled cyber adversaries. However, the Department's layered approach to risk management allows multiple levels of protection. This protection is accomplished by implementing a matrix of technical, operational, and management security controls designed to thwart network threats, detect and mitigate vulnerabilities and strengthen business operations.

In my role as the Chief Information Security Officer, I have become intimately familiar with the benefits, shortcomings and promising opportunities to build upon the current Federal Information Security Management Act of 2002. Our goal is to ensure system security for diplomacy, while continuously improving the return on investment for each dollar spent on cyber security.

The Current Landscape from the Perspective From a Civilian Department

FISMA Benefits. The passage of the Federal Information Security Management Act in 2002 served as a game-changing event for the federal agency community. Whereas, the Health Information Portability and Accountability Act applies to medical information and the Privacy Act of 1974 applies to personal information,

FISMA applies to all information used by or on behalf of the federal department and agency. The establishment of a holistic information security program and the responsibility of accounting to oversight entities, including Congress, served as a valuable check in determining the health of an agency's information security program.

Challenges Faced. The federal cyber landscape has changed over the past five years. The implementation of federal cyber security has typically been implemented through manual processes and compliance checks which have competed with the need to implement Web 2.0 technologies in a secure manner.

Meanwhile our cyber problems have dramatically escalated in severity and frequency. In a typical week, the Department blocks 3.5 million spam e-mails, intercepts 4,500 viruses and detects over a million external probes to our network. Since 2008 the number security related tickets has more than doubled, while malicious code attacks increased by 47%. The volatility of changes to security sensitive settings has been equally problematic.

Recent Trends. In October 2009 the Office of Management and Budget launched CyberScope, a secure, data collection platform for reporting that allows research and analysis across Federal agencies. Additionally, the Federal Chief Information Officer has formed an interagency task force charged with developing metrics for information security. The National Institute of Standards and Technology (NIST) has revised C&A Special Publication 800-37 to increase its emphasis on continuous monitoring, including a recommendation for the use of automation to obtain more timely, cost-effective, and efficient monitoring results. The goal is to give senior leaders better information on the security state of their information

systems with which to make risk-based decisions. For its part, in FY 2009 the Department began supplementing FISMA compliance reports and studies with a risk scoring program scanning every computer and server connected to its network not less than every 36 hours on 8 security factors and twice a month for safe configurations of software.

The Risk Scoring Program utilizes best practices such as the Twenty (20) Most Critical Controls also known as the Consensus Audit Guidelines (CAG); a collaborative effort between government and industry), which we have mapped against the way the Department is being attacked. To assess vulnerabilities, the Department utilizes the National Vulnerability Database (NVD) and the Common Vulnerability Scoring System (CVSS) from NIST and the Department of Homeland Security where scanning tools tag specific risks with point values from 0 to 10, with 10 being the highest vulnerability. For each risk found, an on-line catalog of security related software flaws offers a help kit for the resolution of that particular vulnerability. When the problem is resolved risk points are deducted and a higher score for the technical team and organizations is computed no matter where they are located across the world. To this point, State Department risk scoring program has implemented the sub-set of the 15 Consensus Audit Guideline controls that are susceptible to automated verification.

In the first year of site scoring ending July 2009, overall risk on the Department's key unclassified network measured by the Risk Scoring program was reduced by nearly 90% in overseas sites and 89% in domestic sites. Scores have been relatively stable since then. Notwithstanding this reduction to date, the Department has decided to make it three times more difficult to achieve the same grades by the end of FY 2010 as part of an ongoing commitment to continuous improvement.

These methods, however limited, have allowed one critical piece of the Department's information security program to move from the snapshot in time previously available under FISMA and its related authorities to a program that scans for weaknesses on servers and personal computers– **continuously;** identifies weak configurations – **each 15 days;** recalculates the most important problems to fix in priority order – **daily;** and issues letter grades (A+ to F) **monthly** to senior managers tracking progress for their organization the last 30 days. It is the State Department's objective to expand automated verification to as many CAG and NIST 800-53 controls as possible and to all infrastructure and applications as soon as possible, limited only by available resources.

The various risk score reports tabulate risk scores by region, compare progress overseas to domestic sites, and create an enterprise-wide summary for senior management of the Department. In short, the details empower administrators with targeted, daily attention to conduct remediation and the summaries empower executives to oversee most serious problems.

Other Elements of Cyber Security Defense in Depth at State

In addition to the Risk Scoring program, the Department's layered approach to risk management includes several other noteworthy initiatives.

Network Monitoring & Incident Response

The Department maintains a 24/7 network watch program that guards against the external penetration, compromise, or misuse of the Department's cyber assets. Analysts stationed at our Network Monitoring Center serve as continuous sentries for inappropriate network activity based on intrusion detection system signatures,

reports from the Firewall Team and other sources. The analysts perform preliminary assessments to confirm the nature and source of suspicious network security events. Those matters deemed significant are escalated to the Computer Incident Response Team (CIRT) for in-depth analysis and corrective action.

The CIRT serves as the Department's main clearinghouse for reporting computer security events and incidents occurring on Department and foreign affairs agency networks. CIRT analysts track all reported actions through completion and coordinate incident response actions with all stakeholders including the Department's security units, Department of Homeland Security's US-CERT and law enforcement entities.

This team of technical analysts performs essential coordinated information sharing as defined in NIST Special Publication 800-61. In addition to the reporting requirements found in this publication, Department of State actively communicates on emerging phishing attack threats realized by the Department of State to help other agencies avoid becoming victims of these same phishing scams. Department of state also utilizes, in partnership with US-CERT, the situational awareness initiative EINSTEIN 2 by analyzing and reporting on events detected through this program.

Threat Detection

To combat increasingly sophisticated cyber attacks, the Department's Cyber Threat Analysis Program provides overseas posts and Department management with indicators and early warnings about potential cyber incidents. This team of technical analysts performs essential in-depth assessments of network intrusions

and helps coordinate the Department's response to sophisticated cyber attacks. They also work closely with the law enforcement and network defense communities to develop both a comprehensive threat picture and possible remediation measures. In addition, they perform proactive penetration testing and network forensic analysis to detect and resolve significant threat issues.

Moreover, the Cyber Threat Analysis team has developed a strong information sharing capability by routinely briefing other USG agencies on pressing threat data and offering technical assistance and best practices information in an effort to help mitigate risks to federal networks. In addition, they participate in multiple working groups and information sharing organizations designed to enhance coordination among the government's cyber defense teams.

Global Security Scanning

The Global Security Scanning program of the Department serves multiple essential purposes covering all of its domestic and overseas locations. Electronic tools perform functions that include confirming what is connected to Department networks; assuring that computers, network and software are in the safest configuration of setting, locating system vulnerabilities that need correction and collecting evidence for cyber security investigations. Global scanning is complimented with computer security officers supporting security regionally and locally for overseas posts as "boots on the ground."

Consequences for Cyber Misuse or Abuse

The Department's Cyber Security Incident Program was formed to address consequences for acts of cyber misuse or abuse by individuals. The program enhances the protection of the Department's cyber infrastructure by raising overall

cyber security awareness and providing managers with the ability to hold individual users accountable for acts of cyber misuse or abuse. The Department, like all parts of the federal government, needs to balance the benefits of cyber space for mission effectiveness, with the personal responsibility every employee is asked to demonstrate when using government cyber resources.

The Cyber Security Incident Program applies to all Department system users and defines two different categories of incidents: "infractions", where failure to comply with a specific Department policy exists but does not result in actual damage to the Department's cyber infrastructure and "violations", where failure to comply with a specific Department policy exists and results in damage or significant risk of damage to the Department's cyber infrastructure.

In addition to the types of incidents that lend themselves to detection, the Department's network monitoring and inspections alert key Department officials to risks when they occur. Upon notification of an incident, an investigation is undertaken incorporating several Department organizations charged with gathering the information necessary to ensure a prompt and appropriate response to the cyber event, while protecting the rights of the accused.

Since the Cyber Security Incident Program was established in 2007 a total of 14 users have been cited for infractions and 227 users have been cited for violations. For those found to have committed an infraction or violation, the consequences available to the Department range from a letter of warning, suspension of network access or further disciplinary action.

Other Federal Activity

The Department of State is involved in multiple government-wide efforts that share its IT security solutions with other Departments and Agencies. The most widely use product is an annual IT security awareness course offered to other federal organizations as a Center of Excellence under the Information System Security Line of Business. So far this offering has been delivered to 33,255 federal employees outside the State Department. The State Department is also active in multiple projects with the inter-agency Committee on National Security Systems working on developing common standards for risk studies and authentication of users on networks.

I want to conclude by emphasizing the Department's policies, technology, business processes, and partnerships in place continue to evolve and meet the continuing challenges of the security threats in the cyberspace environment.

I would like to thank the Subcommittee members for this opportunity to speak before you today and would be pleased to respond to any of your questions.

Ms. WATSON. One of the things I wanted to followup with you before we got to questions, I understand that you are considering a kind of Ambassador post within the Department to oversee this. You might want to just speak on it for half a minute before we go on.

Mr. STREUFERT. Yes, ma'am. My immediate responsibilities have to do with the internal networks of the Department of State, but I would be happy to forward any questions that you would have about that legislation to those in our organization that deal with foreign policy aspects of the cybersecurity.

Ms. WATSON. Why don't you just give us a summary of what you have already been considering? That would be information for us.

Mr. STREUFERT. I am sorry, I don't have that information available.

Ms. WATSON. No, you can send it to us.

Mr. STREUFERT. Just send it to you?

Ms. WATSON. Yes.

Mr. STREUFERT. OK, very good. I would be happy to, ma'am.

Ms. WATSON. Thank you so much.

Mr. Wilshusen, we are going to take your testimony and then we are going to recess for about 25 minutes to a half hour. We have four to five votes on the floor. Thank you.

STATEMENT OF GREGORY WILSHUSEN

Mr. WILSHUSEN. Chairwoman Watson, Ranking Member Bilbray, and members of the subcommittee, thank you for the opportunity today to participate in today's hearing on Federal information security.

As we have previously testified, cyber-based threats to Federal systems and critical infrastructure are evolving and growing. Pervasive and sustained cyber attacks continue to pose a potentially devastating threat to the systems and operations of the Federal Government.

Over the past few years, agencies have experienced an increasing number and a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices and controls. While much progress has been made in identifying and implementing these controls, much work remains.

Madam Chair, today I will discuss Federal agencies' efforts to secure their information systems and opportunities to enhance Federal cybersecurity.

For fiscal year 2009, agencies have reported mixed progress in securing their systems and implementing key security activities. For example, although agencies collectively reported providing security awareness training and specialized security training to an increasing percentage of their personnel, they also reported testing the security controls and contingency plans for a decreasing percentage of their systems.

In addition, Federal systems continue to be afflicted by persistent control weaknesses. Most of the 24 major agencies in our review had weaknesses in security safeguards that are intended to control logical and physical access to IT resources, manage the secure configurations of those resources, and ensure the prompt recovery of

service and the continuity of operations should unexpected incidents occur. To illustrate, 21 of 24 major agencies noted inadequate controls over their financial systems were either of significant deficiency or material weakness.

An underlying cause for these weaknesses is that agencies have not yet fully or effectively implemented key elements of their information security programs as required by FISMA. As a result, they remain vulnerable to the unauthorized disclosure and modification of sensitive information and the disruption of mission-critical operations.

Fortunately, opportunities exist to enhance Federal cybersecurity. Agencies can implement the hundreds of recommendations that GAO and agency IGs have made to resolve specific control deficiencies and program shortfalls. Agencies can also expand use of automated tools to perform security functions and increase their efficiency in securing and monitoring networks. These actions will help agencies to better manage the configuration of security features and to prevent, limit, and detect unauthorized access to networks and systems.

In addition, as we have previously recommended, OMB and the workgroup it has convened should develop a balanced set of performance measures that focus on risk and produce better information to gage the status and effectiveness of security efforts. The effective implementation of several Government-wide initiatives can also lead to improved cybersecurity. For example, addressing several challenges we have identified associated with implementing the Comprehensive National Cybersecurity Initiative, which is a collection of 12 projects intended to bolster security on Federal networks, will enhance its chances of success.

Another opportunity is implementing the trusted internet connections EINSTEIN and Federal Desktop Core Configuration Initiatives. These initiatives are intended to consolidate and secure external access points, including those to the Internet; provide network intrusion detection capability; and establish secure configurations for Windows-based workstations. We have ongoing work that addresses the status and implementation of these initiatives.

Finally, opportunities exist to strengthen Federal guidance and the national strategy for cybersecurity. In panel discussions that we hosted, cybersecurity experts identified 12 key improvements that are essential in their view to improving the strategy in our national cybersecurity posture. Consistent with our prior work, implementing these improvements can bolster security of our Nation's most critical Federal and private sector cyber infrastructure.

In summary, Federal agencies continue to tread water in securing their systems and countering the growing and evolving cyber threat. Nevertheless, opportunities exist to improve cybersecurity, but they required a concerted response to ensure that Federal systems are sufficiently safeguarded.

Madam Chair, this concludes my statement. I would be happy to answer any questions.

[The prepared statement of Mr. Wilshusen follows:]

United States Government Accountability Office

GAO

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 2:00 p.m. EDT
Wednesday, March 24, 2010

INFORMATION SECURITY

Concerted Response Needed to Resolve Persistent Weaknesses

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO-10-536T

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-10-536T, a testimony before the Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform, U.S. House of Representatives

Why GAO Did This Study

Without proper safeguards, federal computer systems are vulnerable to intrusions by individuals who have malicious intentions and can obtain sensitive information. The need for a vigilant approach to information security has been demonstrated by the pervasive and sustained cyber attacks against the United States; these attacks continue to pose a potentially devastating impact to systems as well as the operations and critical infrastructures that they support. Concerned by reports of weaknesses in federal systems, Congress passed the Federal Information Security Management Act (FISMA), which authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies.

GAO was asked to testify on federal information security and agency efforts to comply with FISMA. This testimony summarizes (1) federal agencies' efforts to secure information systems and (2) opportunities to enhance federal cybersecurity. To prepare for this testimony, GAO analyzed its prior reports and those from 24 major federal agencies, their inspectors general, and the Office of Management and Budget (OMB).

What GAO Recommends

In previous reports over the past several years, GAO has made hundreds of recommendations to agencies to mitigate identified control deficiencies and to fully implement information security programs.

View GAO-10-536T or key components. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

March 24, 2010

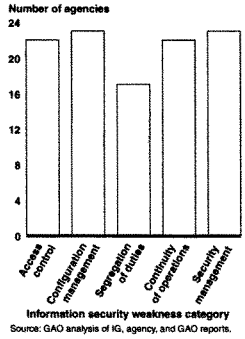
INFORMATION SECURITY

Concerted Response Needed to Resolve Persistent Weaknesses

What GAO Found

Federal agencies have reported mixed progress in securing their systems and implementing key security activities. For example, in fiscal year 2009, agencies collectively reported an increasing percentage of personnel receiving security awareness training and specialized security training, but a decreasing rate of implementation for other key activities when compared to fiscal year 2008. In addition, federal systems continued to be afflicted by persistent control weaknesses. Almost all of the 24 major federal agencies had information security weaknesses in five key control categories, as illustrated in the figure below.

Information Security Weaknesses at Major Federal Agencies for Fiscal Year 2009



Source: GAO analysis of IG, agency, and GAO reports.

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements of an agencywide information security program, as required by FISMA. As a result, they may be at increased risk of unauthorized disclosure, modification, and destruction of information or disruption of mission critical operations. Such risks are illustrated, in part, by the increasing number of security incidents experienced by federal agencies.

Opportunities exist to enhance federal cybersecurity through a concerted response to safeguarding systems that include several components. First, agencies can implement the hundreds of recommendations GAO and inspectors general have made to resolve control deficiencies and information security program shortfalls. In addition, OMB's continued efforts to improve reporting and oversight as recommended by GAO could help assess agency programs. Finally, the White House, OMB, and certain federal agencies have undertaken several governmentwide initiatives that are intended to enhance information security at federal agencies.

Chairwoman Watson and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing on federal information security. As the number of reported computer security incidents and threats to the nation's cyber infrastructure steadily increase, the need for a vigilant and comprehensive approach to federal information security is greater than ever. In 2009, the federal government faced coordinated attacks against its Web sites, and several agencies were affected by the Gumblar Trojan, which uses multiple exploits to compromise legitimate web pages. In addition, the Conficker worm posed a threat to both federal and non-federal systems. Such attacks highlight the importance of developing a concerted response to safeguard federal information systems.

Proper safeguards can mitigate the risk to federal computer systems and networks posed by individuals and groups with malicious intentions. While progress has been made in identifying and implementing these controls, much work remains. Over the past few years, federal agencies 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.

In my testimony today, I will discuss (1) federal agencies' efforts to secure information systems and (2) opportunities to enhance federal cybersecurity. In conducting our review, we analyzed agency, inspector general, Office of Management and Budget (OMB), and our reports on information security. We conducted the review from December 2009 to March 2010 in the Washington, D.C., area in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

To help protect against threats to federal systems, the Federal Information Security Management Act (FISMA)[1] is intended to set 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[2]—assessing risk, establishing a central management focal point, implementing appropriate policies 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 (1) agency heads and chief information officers, to develop, document, and implement an agencywide information security program, among other things; (2) inspectors general, to conduct annual independent evaluations of agency efforts to effectively implement information security; (3) the National Institute for Science and Technology (NIST), to provide standards and guidance to agencies on information security; and (4) 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. In addition, the act 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. FISMA also requires OMB to report annually to Congress by March 1.

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

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

Although Agencies Report Mixed Progress, Deficiencies in Information Security Controls Remain

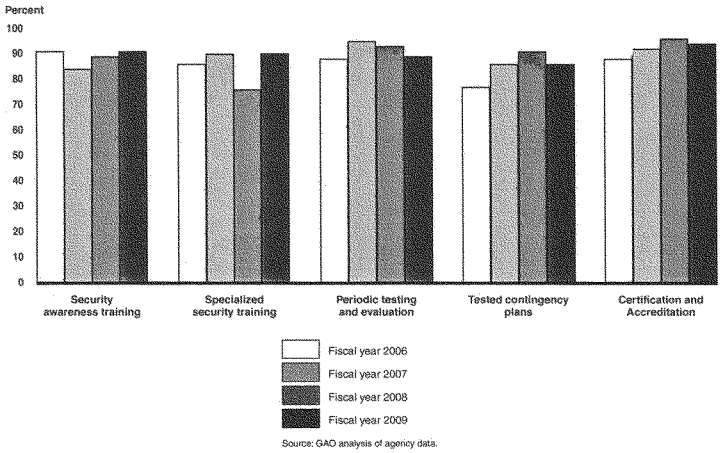
FISMA requires each agency, including agencies with national security systems, to develop, document, and implement an agencywide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. As part of its oversight responsibilities OMB requires agencies to report on specific performance measures, including:

- Percentage of employees and contractors receiving IT security awareness training,
- Percentage of employees with significant security responsibilities who received specialized security training,
- Percentage of systems whose controls were tested and evaluated,
- Percentage of systems with tested contingency plans, and
- Percentage of systems certified and accredited.

Since the enactment of FISMA in 2002, federal agencies have generally reported increasing rates of implementation for key information security activities. However, in fiscal year 2009, agencies reported mixed progress in implementing these activities compared to fiscal year 2008. For example, governmentwide, agencies collectively reported that 91 percent of employees and contractors had received security awareness training in fiscal year 2009, up from 89 percent in fiscal year 2008. Agencies also reported that 90 percent of employees with significant information security responsibilities had received specialized training, up from 76 percent in fiscal year 2008.

In other key areas, agencies reported slight decreases from fiscal years 2008 to 2009. Specifically, the percentage of systems for which security controls have been tested and reviewed decreased from 93 percent to 89 percent, the percentage of systems with tested contingency plans decreased from 91 percent to 86 percent, and the percentage of systems certified and accredited decreased from 96 percent to 94 percent. A summary of these percentages is shown in figure 1.

Figure 1: Selected Performance Metrics for Agency Systems



Source: GAO analysis of agency data.

In these and other areas, inspectors general at the 24 major agencies have also reported weaknesses in their fiscal year 2009 audits and evaluations. Weaknesses in requirements such as periodic testing and evaluation, certification and accreditation, configuration management, and remedial actions were most commonly reported. For example,

- at least 13 inspectors general reported that their agencies had insecure configuration settings, or had not applied needed patches in a timely manner, or both;
- at least 15 inspectors general reported that their agency did not adequately assess security controls such as those recommended by NIST;
- at least 11 inspectors general reported that their agencies failed to create a remediation plan for all identified weaknesses.
- at least 13 inspectors general reported that documents required to make an informed decision regarding certification and accreditation of systems

were either missing or incomplete, or that the accreditation was allowed to expire on at least one system without recertification;

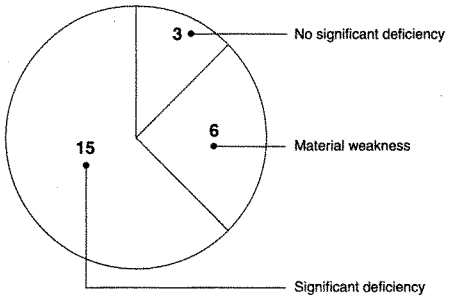
Weaknesses such as these continue to impair the government's ability to ensure the confidentiality, integrity, and availability of critical information and information systems used to support the operations and assets of federal agencies. Until these agencies fully implement information security requirements, they may be at increased risk of unauthorized disclosure, modification, and destruction of information or disruption of mission critical operations.

Despite Reported Progress, Federal Systems Remain Vulnerable

GAO and agency inspectors general reviews continue to highlight deficiencies in the implementation of security policies and procedures at federal agencies. In their fiscal year 2009 performance and accountability reports, 21 of 24 major agencies noted that inadequate information system controls over their financial systems and information were either a material weakness or a significant deficiency (see fig. 2).[3]

[3]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 for Financial Reporting



Source: GAO analysis of agency performance and accountability report, annual financial report, or other financial statement reports for FY 2009.

Our audits and those of the inspectors general continue to identify similar conditions in both financial and non-financial systems. Most of the 24 major federal agencies had reported deficiencies in the following major categories of information security controls, as defined by our *Federal Information System Controls Audit Manual*:[4]

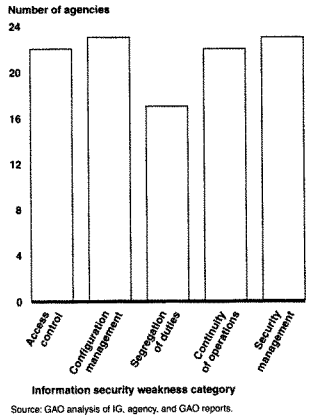
- access controls, which ensure that only authorized individuals can read, alter, or delete data;
- configuration management controls, which provide assurance that only authorized software programs are implemented;
- segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection;
- continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and

[4]GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G (Washington, D.C.: Feb. 2009).

- an agencywide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented.

As shown in figure 3, agencies reported deficiencies in all five of the information security control areas. For example, agencies did not consistently configure network devices and services to prevent unauthorized access and ensure system integrity; assign incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction; and maintain or test continuity of operations plans for key information systems. Such information security control weaknesses unnecessarily increase the risk that the reliability and availability of data that are recorded in or transmitted by federal systems could be compromised.

Figure 3: Number of Major Agencies Reporting Weaknesses by Control Category for Fiscal Year 2009



Source: GAO analysis of IG, agency, and GAO reports.

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements of an agencywide information security program, as required

by FISMA. An agencywide security program provides a framework and continuing cycle of activity that includes 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. According to inspector general, agency, and our previous reports, 23 of the 24 major federal agencies had weaknesses in their agencywide information security programs.

The following examples, reported in 2009, illustrate that a broad array of federal information and systems remain at risk.

- At the Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of the Treasury, key information security program activities were not implemented.[5] For example, FinCEN did not always include detailed implementation guidance in its policies and procedures or adequately test and evaluate information security controls.
- The information security program for the classified computer network at the Los Alamos National Laboratory (LANL) had not been fully implemented.[6] Specifically, (1) risk assessments were not comprehensive, (2) specific guidance was missing from policies and procedures, (3) the training and awareness program did not adequately address specialized training needs for individuals with significant network security responsibilities, (4) system security plans were incomplete, (5) the system security testing and evaluation process had shortcomings, (6) corrective action plans were not comprehensive, and (7) contingency plans were incomplete and not tested. In addition, the laboratory's decentralized management approach has led to weaknesses in the effectiveness of its classified cybersecurity program. Although the laboratory has taken steps to address these weaknesses, its efforts may be limited because LANL has not demonstrated a consistent capacity to sustain security improvements over the long term.

[5]GAO, *Information Security: Further Actions Needed to Address Risks to Bank Secrecy Act Data*, GAO-09-195 (Washington, D.C.: Jan. 30, 2009).

[6]GAO, *Information Security: Actions Needed to Better Manage, Protect, and Sustain Improvements to Los Alamos National Laboratory's Classified Computer Network*, GAO-10-28 (Washington, D.C.: Oct. 14, 2009).

- We identified a number of shortcomings in key program activities at the National Aeronautics and Space Administration (NASA).[7] For example, NASA had not always (1) fully assessed information security risks; (2) fully developed and documented security policies and procedures; (3) included key information in security plans; (4) conducted comprehensive tests and evaluation of its information system controls; (5) tracked the status of plans to remedy known weaknesses; (6) planned for contingencies and disruptions in service; (7) maintained capabilities to detect, report, and respond to security incidents; and (8) incorporated important security requirements in its agreement with its contractor.

In addition, the inspectors general at 13 of the 24 major agencies reported information security as major management challenge. 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; a designation we have made in each report since 1997.[8]

Reported Security Incidents Are on the Rise

Consistent with the evolving and growing nature of the threats and persistent vulnerabilities to federal systems, agencies are reporting an increasing number of security incidents and events. These incidents put sensitive information at risk. Personally identifiable information about Americans has been lost, stolen, or improperly disclosed, thereby potentially exposing those individuals to loss of privacy, identity theft, and financial crimes. Reported attacks and unintentional incidents involving critical infrastructure systems demonstrate that a serious attack could be devastating. 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.

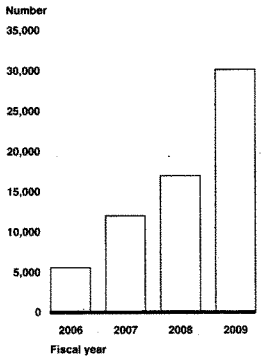
When incidents occur, agencies are to notify the federal information security incident center—the United States Computer Emergency Readiness Team (US-CERT). US-CERT serves as a focal point for the government's interaction with federal and nonfederal entities on a 24-hour-a-day, 7-day-a-week basis regarding cyber-related analysis, warning,

[7]GAO, *Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks*, GAO-10-4 (Washington, D.C.: Oct. 15, 2009).

[8]Most recently, GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

information sharing, major incident response, and national-level recovery efforts. As shown in figure 4, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 4 years, increasing from 5,503 incidents reported in fiscal year 2006 to about 30,000 incidents in fiscal year 2009 (over a 400 percent increase).

Figure 4: Incidents Reported to US-CERT, FY 2006-2009



Source: GAO analysis of US-CERT data.

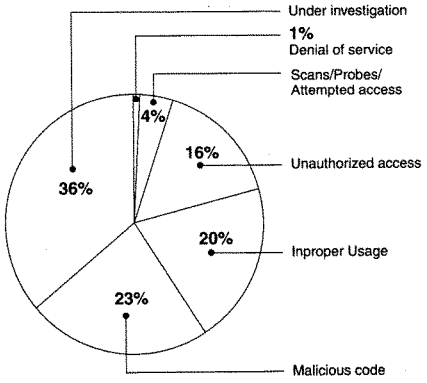
Agencies report the following types of incidents and events based on US-CERT-defined categories:

- **Unauthorized access:** Gaining logical or physical access without permission to a federal agency's network, system, application, data, or other resource.
- **Denial of service:** Preventing or impairing the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim of or participating in a denial of service attack.
- **Malicious code:** Installing malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus software.

- **Improper usage:** Violating acceptable computing use policies.
- **Scans/probes/attempted access:** Accessing or identifying a federal agency computer, open ports, protocols, service, or any combination of these for later exploit. This activity does not directly result in a compromise or denial of service.
- **Unconfirmed incidents under investigation:** Investigating unconfirmed incidents that are potentially malicious, or anomalous activity deemed by the reporting entity to warrant further review.

The four most prevalent types of incidents and events reported to US-CERT during fiscal year 2009 were: (1) malicious code comprising 23 percent; (2) improper usage, 20 percent; (3) unauthorized access, 16 percent; and (4) unconfirmed incidents under investigation, 36 percent. Incidents reported to US-CERT in fiscal year 2009 are shown by type in figure 5.

Figure 5: Percentage of Incidents Reported to US-CERT in Fiscal Year 2009 by Category



Source: GAO analysis of U.S. CERT data.

Opportunities Exist for Enhancing Federal Cybersecurity

A concerted response to safeguarding federal systems includes several components. Agencies can take action to resolve specific security weaknesses, federal law and guidance can be strengthened, and continued effort can be made on governmentwide security initiatives.

Over the past several years, we and agency inspectors general have made hundreds of recommendations to resolve significant control deficiencies and information security program shortfalls. Effective implementation of our recommendations will help agencies to prevent, limit, and detect unauthorized access to computerized networks and systems and help ensure that only authorized individuals can read, alter, or delete data. In addition, implementation of these recommendations will help agencies to better manage the configuration of security features for hardware and software and assure that changes to the configuration are systematically controlled.

We have also recommended that agencies fully implement comprehensive, agencywide information security programs, including by correcting weaknesses in specific areas of their programs such as: (1) assessments of the risk to information systems; (2) information security policies and procedures; (3) planning for interruptions to information system processing; (4) training personnel in awareness of security policies and procedures; (5) periodic tests and evaluations of the effectiveness of information system controls; and (6) the implementation of plans of action to remediate information security weaknesses. The effective implementation of these recommendations will strengthen the security posture at these agencies. Agencies have implemented or are in the process of implementing many of our recommendations.

In addition, agencies can also increase their efficiency in securing and monitoring networks by expanding their use of automated tools as part of their monitoring programs for performing certain security-related functions. Because federal computing environments are very large, complex, and geographically dispersed, often consisting of tens or hundreds of thousands of devices, increasing automation of key security processes can assist in the efficient and effective implementation of key controls across the entire enterprise. For example, agencies can better use centrally administered automated diagnostic and analytical tools to continuously scan network traffic and devices across the enterprise to identify vulnerabilities or anomalies from typical usage and monitor compliance with agency configuration requirements. In addition, improving the use of automated tools for patch management can increase

efficiency in mitigating known vulnerabilities on many systems within an agency.

Strengthen FISMA and Its Implementing Guidance

FISMA was intended to provide (1) a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets and (2) a mechanism for improved oversight of federal agency information security programs. In June 2009,[9] we proposed several suggested actions that could improve FISMA and its associated implementing guidance, including (1) clarifying requirements for testing and evaluating security controls; (2) requiring agency heads to provide an assurance statement on the overall adequacy and effectiveness of the agency's information security program; (3) enhancing independent annual evaluations; (4) strengthening annual reporting mechanisms; and (5) strengthening OMB oversight of agency information security programs. Implementing these suggestions can improve the implementation and oversight of federal agency information security programs.

Continue Efforts to Improve Reporting and Oversight

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 preparing the annual FISMA reports. OMB developed an online reporting tool during fiscal year 2009 to improve the efficiency of the annual reporting process. Agencies are required to use the online tool to submit their annual reports and OMB is to use the data submitted in its online reporting tool to summarize 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 its annual reporting instructions and oversight.[10] For example, we have recommended that OMB update its annual reporting instructions to request inspectors general report on the effectiveness of agencies'

[9]GAO, *Federal Information Security Issues*, GAO-09-817R (Washington, D.C.: June 30, 2009).

[10]GAO, *Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses*, GAO-09-546 (Washington, D.C.: July 17, 2009) and *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, GAO-07-837 (Washington, D.C.: July 27, 2007).

processes for developing inventories, monitoring contractor operations, and providing specialized security training. OMB has acted to enhance its reporting instructions; however, further actions need to be taken to fully address these recommendations.

We have also recommended that OMB develop metrics that (1) focus on the effectiveness of information security controls and (2) the overall impact of an agency's information security program.[11] In September 2009, OMB convened a Security Metrics Taskforce to develop new FISMA performance measures. According to OMB's website the taskforce is comprised of officials from the both the federal community and private sector and was tasked with developing metrics that focus on outcomes rather than compliance that agencies will be required to report as part of the FISMA reporting process. In December 2009, OMB released draft metrics for comment but has not yet released the final metrics.

Continue to Enhance Federal Information Security through Governmentwide Initiatives

The White House, OMB, and certain federal agencies have undertaken several governmentwide initiatives that are intended to enhance information security at federal agencies.

Address challenges in implementing CNCI. In January 2008, President Bush established the Comprehensive National Cybersecurity Initiative (CNCI). The initiative, which consists of 12 projects, is intended to reduce vulnerabilities, protect against intrusions, and anticipate future threats against federal executive branch information systems.[12] As we recently reported,[13] the White House and federal agencies have established interagency groups to plan and coordinate CNCI activities. However, CNCI faces challenges in achieving its objectives related to securing federal information, including better defining agency roles and responsibilities, establishing measures of effectiveness, and establishing an appropriate level of transparency. Until these challenges are adequately addressed, there is a risk that CNCI will not fully achieve its goals. Among other

[11]GAO, *Information Security: Concerted Effort Needed to Improve Federal Performance Measures*, GAO-09-617 (Washington, D.C.: Sep. 14, 2009).

[12]The White House, National Security Presidential Directive 54/ Homeland Security Presidential Directive 23 (Washington, D.C.: Jan. 8, 2008).

[13]GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, GAO-10-338 (Washington, D.C.: March 5, 2010).

recommendations, we recommended that the Director of OMB take action to: (1) better define roles and responsibilities of all key CNCI participants; (2) establish measures to determine the effectiveness of CNCI projects in making federal information systems more secure and track progress against those measures; (3) establish an appropriate level of transparency about CNCI; and (4) reach agreement on the scope of CNCI's education projects to ensure that an adequate cadre of skilled personnel is developed to protect federal information systems. OMB agreed with 3 of the 4 recommendations, disagreeing with the recommendation regarding defining roles and responsibilities. However, such definitions are key to achieving CNCI's objective of securing federal systems.

Continue efforts to implement TIC and Einstein initiatives. Two specific initiatives of CNCI are Trusted Internet Connections (TIC) and Einstein. TIC is an effort to consolidate the federal government's external access points (including those to the Internet). TIC is also intended to establish baseline security capabilities and validate agency adherence to those security capabilities. The Einstein initiative is a computer network intrusion detection system that analyzes network flow information from participating federal agencies. The system is to provide a high-level perspective from which to observe potential malicious activity in computer network traffic of participating agencies' computer networks. Einstein is intended to alert US-CERT in real time of this activity and provides correlation and visualization of the derived data. We have ongoing work that addresses status and implementation of these initiatives.

Continue efforts to implement FDCC. Under the Federal Desktop Core Configuration Initiative, OMB directed agencies that have Windows XP and/or Windows Vista operating systems deployed to adopt the security configurations developed by the National Institute of Standards and Technology, the Department of Defense, and DHS. The goal of this initiative is to improve information security and reduce overall information technology operating costs. We have ongoing work that addresses status and implementation of this initiative.

Improve the national strategy for cybersecurity. In March 2009, we testified on needed improvements to the nation's cybersecurity strategy.[14]

[14]GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, GAO-09-432T (Washington, D.C.: March 10, 2009).

In preparation for that testimony, we obtained the views of experts (by means of panel discussions) on critical aspects of the strategy, including areas for improvement. The experts, who included former federal officials, academics, and private sector executives, highlighted 12 key improvements that are, in their view, essential to improving the strategy and our national cybersecurity posture. The key strategy improvements identified by cybersecurity experts are listed in table 1.

Table 1: Key Strategy Improvement Identified by Cybersecurity Experts

1. Develop a national strategy that clearly articulates strategic objectives, goals, and priorities.
2. Establish White House responsibility and accountability for leading and overseeing national cybersecurity policy.
3. Establish a governance structure for strategy implementation.
4. Publicize and raise awareness about the seriousness of the cybersecurity problem.
5. Create an accountable, operational cybersecurity organization.
6. Focus more actions on prioritizing assets, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.
7. Bolster public-private partnerships through an improved value proposition and use of incentives.
8. Focus greater attention on addressing the global aspects of cyberspace.
9. Improve law enforcement efforts to address malicious activities in cyberspace.
10. Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate government and private sector efforts.
11. Increase the cadre of cybersecurity professionals.
12. Make the federal government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services.

Source: GAO analysis of opinions solicited during expert panels.

These recommended improvements to the national strategy are in large part consistent with our previous reports and extensive research and experience in this area. Until they are addressed, our nation's most critical federal and private sector cyber infrastructure remain at unnecessary risk to attack from our adversaries.

Since our March testimony, the Obama Administration has performed a review[15] of the strategy and issued a list of short and long term actions,

[15]The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C.: May 29, 2009).

which are largely consistent with our past reports and recommendations, to strengthen the strategy. In response to one of these actions, the president appointed a cybersecurity coordinator in December 2009. We recently initiated a review to assess the progress made by the executive branch in implementing the report's recommendations.

In summary, while federal agencies continue to report increased compliance in implementing security training requirements, most federal agencies reported weaknesses in most types of information security controls. Additionally, agencies reported mixed progress in implementing key security measures while inspectors general identified persistent weaknesses in those areas of agencies' information security programs. There are multiple opportunities for the federal government to enhance federal cybersecurity and address these continuing weaknesses. These opportunities include addressing the hundreds of recommendations we and inspectors general have made to agencies, making enhancements to FISMA and its implementing guidance, and continuing efforts on White House, OMB, and federal agencies' initiatives. A concerted response by the federal government to current information security challenges will include acting on these opportunities; without such a response, federal information and systems will remain vulnerable.

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 statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include Anjalique Lawrence (Assistant Director), Larry Crosland, Sharhonda Deloach, Kristi Dorsey, Rebecca Eyler, Nicole Jarvis, Linda Kochersberger, Mary Marshall, Minette Richardson, and Jayne Wilson.

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

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Please Print on Recycled Paper

Ms. WATSON. Thank you so very much, panel. We will recess now until about 3:45, and we will see you back here for questions and then panel two. Thank you so very much.

[Recess.]

Ms. WATSON. We shall resume the committee.

I was listening very intently to Mr. Kundra's report, and you mentioned Mr. Howard Schmidt, the new White House Cyber Coordinator, while you were testifying. Could you describe for us what his role and responsibilities are in securing our Federal information infrastructure? As you know, my legislation calls for the codification of a National Office of Cyberspace and Grants, and its extensive authority for implementing and enforcing information and security responsibilities. So we would like to know more about Mr. Schmidt's role. Thank you.

Mr. KUNDRA. Sure. Howard Schmidt, as the coordinator of cybersecurity within the White House, works both at the National Security Council and the National Economic Council, recognizing that their vital interests in terms of being able to protect the Nation, at the same time making sure we are balancing that with economic decisions across the board.

Also, when you think about from a national security perspective, the Comprehensive National Cyber Initiative, both of us work very, very closely together to make sure that, as we look at equities, whether it is the Department of Defense, Homeland Security, the private sector, that we are coordinating our efforts and are moving forward in a direction that makes us more secure, rather than spending a tremendous amount of energy on the friction that results historically from a lack of coordination and who owns cybersecurity in one area versus the other.

Ms. WATSON. One proposal in my bill requires OMB to incorporate secure product and service acquisition requirements into agency contracting practices, as well as to require IT investments to have vulnerability assessments completed before programs can move forward. So can you tell us how these proposals are complementary to some programs already in place at GSA and what you might consider to be technical barriers that we might be able to remove?

Mr. KUNDRA. Part of what we need to be able to do across the Federal Government is not bolt on security afterwards. A lot of times what ends up happening is systems end up going live or they evolve. Some of the systems may be 30 years old and everybody is trying to bolt on security, and the challenges as addressed by the panel, with a huge focus on generating a lot of reporting.

And if we looked at the FISMA report, one of the key findings here is investments we are making when it comes to the human capital side, making sure that employees who are focused on cybersecurity across the public sector are not necessarily experts in writing reports, but are actually people who are trained and understand how to not just configure and manage routers and switches and servers and desktops and firewalls, but can make sure that as we deploy these systems we build an architecture that doesn't say, you know what, we are going to move forward and certify this system, and come back 3 years from today and hope that it is as se-

cure, test it. What we are trying to shift everyone to is this notion of a continuous monitoring.

But what we are also doing is we are making sure that across the board, in terms of procurements, that we are creating schedules where you have enterprise procurements, whether it is moving toward a networks contract or whether it is blanket purchase agreements for software, whether it is any virus or firewalls or data loss prevention technologies, so that it is easier to procure these technologies and, from an OMB perspective, for us to be able to look at where we are actually spending money. And, frankly, security investments are best when they are actually baked into the systems that we are looking at and not where they are treated at discreet investments cross the board.

Ms. WATSON. Can you describe what actually is working? I think we know that there are firewalls in some agencies that are lax, but what is actually working today?

Mr. KUNDRA. What is working right now is—let's look at Homeland Security Presidential Directive around HSPD–12, which is smart cards, the issuance of these smart cards across the board. What we have been able to do in this year alone, we have seen a 60-plus percent rise in the issuance of these smart cards because we focused on it. We have had these accountability sessions that we call text ed sessions——

Ms. WATSON. Now, the smart card you are talking about, who has that card? How is it distributed? Where is it and where is it given?

Mr. KUNDRA. The way these smart cards work, they are actually designed to be able to be given to Federal employees and contractors who work on Government systems. And part of what we are trying to do now is that the issuance of these cards has moved forward. In the Department of Defense, for example, these cards are used to actually log into some of the systems. And what we are trying to do is make sure that across the Federal Government—here is one of these smart cards——

Ms. WATSON. Wait a minute. Do you have a fingerprint on that and a mug shot?

Mr. KUNDRA. As well as a photograph, there is a chip, there are a couple of bar codes and there is some imagery.

Ms. WATSON. I mean, can someone really hack in and change that and steal your identify through those?

Mr. KUNDRA. And that is why these smart cards are very, very important, because one of the challenges we also face is making sure that the very people who are accessing our systems, we know who they are, we know when they are logging into the systems, we know what information they are getting access to. So this initiative is successful. Now what we need to do is sort of the second part of this, which is hard work on making sure that every single agency across the Federal Government is not just issuing these cards, but actually making sure that the systems are configured to be able to use these cards.

DOD has done a good job in this area. A number of other agencies have moved forward in making sure they are integrating them. But the vision here is to also make sure that we are using these smart cards for physical access, which is getting in and out of

buildings, and logical access, which is getting in and out of systems across the Federal Government.

Ms. WATSON. And using these cards and the information that we have, what bothers me is that we still have a barrier in communicating. You know, I am still wrapped up in what happened on Christmas Day and why our Secretary did not know that there was someone getting on a plane in another country, entering our airspace and being a tremendous threat. Thank God they caught him, but what happens there? Why isn't that information communicated?

Mr. KUNDRA. Part of what is also happening within information sharing environment is making sure that across the board, across Federal systems that they are configured not just to share information from a technical perspective, but also from a management perspective, recognizing that this is not necessarily a technical problem; recognizing what are the important things that we need to focus on, what is the information that is vital, and how do we simply so we recognize as we see these threats.

What is really interesting from a security perspective, as John testified, from the State Department's perspective, how they are able to look at certain—create certain grades across the different embassies and figure out where are they secure versus where are they not secure so they can focus their attention, their energy, and finite resources on the highest priority problems. The only way we are going to be able to attack cybersecurity is by focusing—sort of the 80/20 rule, focusing on 80 percent of the problems that we recognize are confronting us today as we think long-term about how do we get to 100 percent.

The challenge we have is that our adversaries are constantly evolving. The threat is a real-time threat and we are constantly seeing the threat vectors change over time. That is why, when we think about our research and development agenda, it is vital, as we look at our R&D agenda, to make sure that we are making investments that are going to yield dividends down the line to shift the advantage so that the defender has a greater opportunity rather than the attacker, because the attacker has to get it right once.

Ms. WATSON. I am going to yield now to the ranking member, Mr. Bilbray.

Mr. BILBRAY. Thank you, Madam Chair.

Mr. Kundra, while I have you before us, there is something that just sort of came up, and that is this issue of information sharing, whatever. I am sure you read the 9/11 Commission report about the firewalls that created the opportunity for people to actually move within the United States, and though information was available with one department, the other department didn't have any access in it; and that was actually probably more statutory than it was a problem of the incapability of systems.

You are aware of the 9/11?

Mr. KUNDRA. Yes, sir.

Mr. BILBRAY. OK. Because one of the things that really ought to be a lesson for us on this, as we bring this up, Madam Chair, is a member of the 9/11 terrorists—not the 9/11 terrorists, but the D.C. sniper, where you had a fingerprint that was detected at a murder site in Alabama. Except for one little incident we never

would have been able to catch this individual because even though we had all of his fingerprints, but the fact that one department was not allowed to have access into another department, we had those firewalls, and it is something the 9/11 really said we needed to point to. And I just tell you that. Luckily, the 9/11 terrorists had committed a misdemeanor which allowed his immigration fingerprints and biometrics to be brought over to the FBI, so then when the Alabama officer asked to check the fingerprints, we were able to have access.

The question is this: How many crimes and stuff are going on right now because not just Homeland Security isn't sharing it, but a lot of other agencies may have information and data that can't be shared now? I just ask you to take a look at that. 9/11 has said it. We haven't done enough about that. But information sharing and tearing down those firewalls are something we haven't done enough of, and I ask you to look at that.

The other question is again—and we brought it up, and maybe it is overplayed and whatever, and that is the securing of not only through different systems, but the biometrics are one thing we can talk about.

One of the things that we had a hearing today about is legislation about telecommuting and this issue of computers being able to be accessed through the internet. Can you talk to me about the challenges you see there, like what happened to Snowmageddon here, when we started having people working at home during that period but using the Internet to access? We basically have to say there are certain people that just cannot be allowed to work over the Internet in this issue. Comments? Let me just open it up.

Mr. KUNDRA. Sure. A part of what we want to be able to do in the broader context of deploying technology is make sure that, on the one hand, we are leveraging innovation; whether that is mobile technology in terms of cell phones and PDAs that allow you to have access to real-time information or telecommuting, for that matter. And as we think about the Federal Government and where we are headed, whether the investments we are making in cloud computing or the shift toward where we want to be able to attract the best and brightest people across the country, is recognizing that there are inherent risks, but at the same time addressing and confronting those risks.

So if we look at telecommuting, for example, GSA had significant number of employees who were telecommuting. The Patent and Trademark Office, on a regular basis, has a significant number of employees telecommuting. So does the GAO, which is one of the leaders of the Government in terms of telecommuting.

But what we need to be able to do is make sure, like with the smart card, being able to authenticate people across those systems; and these artificial boundaries that we had before in the Federal Government, where we believed you could build a citadel and walls around a system, in the new computing paradigm, unfortunately, security is going to have to be baked in at the data element layer, protecting every piece of data. And part of what CIOS and Chief Information Security Officers across the Federal Government are dealing with is figuring out how do we, on the one hand, leverage

these technologies and, on the other hand, make sure that we are providing the appropriate security controls.

And I am sure Gus and John can comment on this too, given that they have missions that are not necessarily just within the United States, but all over the world, and addressing security in the global context.

Mr. BILBRAY. Comments, gentlemen?

Mr. GUISSANIE. Yes, sir. That is a very interesting example. The issue with telecommuting back into an organization's information system is if you are using, for instance, a DOD laptop and you take that home and you use your broadband connection to come back into DOD, we can do that securely; we can establish a secure link using your broadband connection. We trust the computer you have because we gave it to you, and that makes to fairly safe for you to essentially work from home. The trouble we have is people don't always have the resources to provide the laptop. In many places in DOD the laptop has become the desktop, so it is pretty easy to use; other places they haven't.

The problem with using the home computer, which lots of folks advocate—why can't they just telecommute from their home computer—is the home computer probably isn't very secure. Somebody has been out on the internet doing things and visiting various sites and they have picked up viruses and malware, and now they turn around and try to get into the Department's information system and I have a problem.

So we have been looking at virtualization technology in the Department for a way to kind of get around that problem, and that essentially means establishing a little virtual environment that is safe and secure on a platform like your home computer that is isolated from the bad kind of malware that might be on that computer.

So in preparation for the pandemic that we all anticipated we might encounter this year, the Department looked at how to do that on a widespread basis. So we came up with a CD-ROM that we called a boot disc, and it contained a mini operating system and it would work on both an Apple computer and a Microsoft-based computer, and you could take it home and it would load up onto the RAM and create its own little virtual environment, and it could only go to one place. It would understand what network it was supposed to connect to. It would allow me to securely authenticate with my smart card into the network and then you could essentially run it just off remote desktop, just like it was on your office computer. When you were finished, nothing was left, no residue was left on the home computer, so there is nothing sensitive there for anybody to find, and because you created that virtual environment, there wasn't any way that somebody who was sitting on that computer that shouldn't be could get into the Department.

So we didn't have a pandemic, but those discs were used, I understand, quite extensively during Snowmageddon, and we had quite a success in people being able to telecommute because they had the disc sitting there.

Mr. BILBRAY. I am glad to hear that. What I worry about when we talk about the smart card, I look at the Pentagon and worry that we are using the same pass card, access card that we did in

9/11, with no biometric confirmation. Are we looking at the smart card utilizing biometric confirmation so not just somebody with the card, but somebody with the right biometrics? In other words, when you steal the card, you better steal the index finger too, right?

Mr. GUISSANIE. Yes, sir. Currently, the smart cards we have are two-factor authentication: the smart card itself, which has some things in it, and then there is a PIN that you have to know to make that work. The three-factor authentication would be something you are, for instance, a thumb print. So we have been looking at that. Currently, the cost and the technology is a little bit prohibitive to make that work when I have to issue 4 million cards out, but we are approaching that. So that way it is the PIN, your thumb print makes it active, they know it is you, and then the technology, the cryptography on the card allows that to establish a secure connection.

Mr. BILBRAY. Do you realize since 1978 the California driver's license has had the ability to use biometric confirmation?

Mr. GUISSANIE. No, sir, I was not aware of that.

Mr. BILBRAY. That is why every time we go in to get our license renewed, they get one more fingerprint on us.

Thank you very much, Madam Chair.

Ms. WATSON. Yes. I would like to go to Mr. Streufert now and ask about your risk scoring program. Can you summarize for us the key technical administrative and physical controls or elements of this program that have enabled State to have such a significant reduction in its cyber risk profile? I am very concerned about the decentralization nature of our embassies, our bureaus, and our consulates. How is State able to manage the implementation of the FISMA security requirements? So if you could kind of expand on that.

Mr. STREUFERT. Yes, Madam Chairwoman. We use the scanners that we have had available for a number of years to turn out the three-ring binder reports for the Federal Information Security Management Act and we decided that the frequency of doing those reports every 3 years was just not enough for us, along the lines of my testimony that our number of malicious code attacks has increased by 47 percent. So we set about a task of trying to increase that frequency and we found that we could physically go in and collect the things instead of once every 3 years, we could collect it every 15 days.

And on another set of factors, eight of them, we could actually do not less than every 36 hours to the far reaches of the planet, let's say to Colonia, the capital of Micronesia, where you were the Ambassador. So by collecting that information—and I checked again this morning—we can find any particular problem on any of the workstations in the embassy that you used to watch and total up what is the average risk for each of those personal computer devices and the server which helps the operations of the embassy. And we can duplicate that across all 260 embassies and our some 100 locations in the domestic United States.

So that information comes back to a central point and we are able to not only assess the risk for each location and how they stack up against their counterparts, but also look at trends. So

when the recent attack that occurred, the so-called Google virus, we knew where that was in our organization and we charged 40 points the first week when that wasn't taken care of, and the second week we charged 80 points for it, the third week we did 120, the following week we did 160. You can see the trend.

We are now up to 320 negative points for not getting on top and fixing that virus as fast as we should. And we can tell you across our entire organization where it has been done and not done, and after a point, if they don't take care of business, it turns like elementary school into a C, D, or F, and that report goes to the Ambassador, the assistant secretary, and that calls for a little closer inspection on the part of the people that do security in our Department.

Ms. WATSON. Well, are we training our consular officers up on all of this? Because my concern, when we put Homeland Security together, you know, 750,000 employees under this umbrella, and I felt that the consular corp should not go underneath it; it should stand alone in the State Department, because they have a very specialized set of skills. So I am wondering how is it working out under Homeland Security and that particular set of skills. I mean, are you training up your consular officers out in the embassies?

Mr. STREUFERT. Well, we try. The functions that I am most familiar with are the information systems support for software applications that might help in the managing of passports and visas. Everyone in the organization, no matter what embassy they are, have access to these reports and what their progress is, and we ran statistical reports on whether it was a large embassy or a small one like Colonia, and we found that really the most important factor was to get the critical security information in the hands of the people that could make a difference.

So for those that work directly for the Department of State, we are able to find out what the situation is, and we have not in fact had serious training problems. In fact, what we found is that this system uses the time more efficiently of our security professionals. So whereas we used to have about 60 people who wrote certification and accreditation reports, by the time we implemented this system, we estimate that there are 4,135 people with significant security responsibilities that are protecting our infrastructure.

Now, I have to say that at the moment we are concentrating on servers and personal computers. There are many aspects of the Consensus Audit Guidelines that we have not yet reached, like our routers and firewalls and some of those other items. So the State Department has a beginning on this, but I won't say that there aren't quite a few things that we yet need to work on.

Ms. WATSON. I am really pleased that we are having this hearing today, and I want Mr. Bilbray to really know that we are trying to improve on our cyber management, and I am pleased to hear what the State Department is doing, because I do know that out there in these remote embassies you don't necessarily get updated on what is available to you, and the training is not always available to these people. And I thought, oh, my goodness, putting them under Homeland Security will just complicate. So I am glad you are aware and that you are actually doing something about it.

Let me go very quickly to Mr. Greg Wilshusen. Your testimony states that for fiscal year 2009, 36 percent of all cyber incidents reported to US-CERT at DHS are still under investigation. Can you summarize what the largest categories of incidents reported were and what the statistics tell us about future or emerging threats?

Mr. WILSHUSEN. Yes, I would be glad to. Based upon our analysis of the information that agencies are required to report to the US-CERT, this year, for fiscal year 2009, the number of incidents increased tremendously, from about 16,800 in fiscal year 2008 to just about 30,000 for fiscal year 2009. Of those, four key categories of these incidents include unauthorized access in which an individual was able to gain unauthorized access to an information or to a system; improper usage, that is when the acceptable use policies of that system or network was inappropriately used; and malicious code, and that is a key one, too.

That was comprised of about 23 percent of all of the incidents and events reported to US-CERT, and that is when a Trojan or malicious software was actually installed on a computer. And then the biggest area had to do with those incidents that are still under investigation, and those are ones in which it is suspected that an incident or an event has occurred, but the extent of it or the character of that incident had not yet been fully determined. So agencies were required to go ahead and report that and they are still under investigation by those agencies.

Ms. WATSON. OK, I would like now to ask our ranking member if he has a question.

Mr. BILBRAY. Yes. I just want to make sure that I don't pass the representative from the State Department. You know, we talk about a lot of things, but I think one of the great successes is the VISIT system. Huge data acquired. I mean, it is astonishing how much data has gone through there. If publicly you can talk about it, have we had any problems with unauthorized access into that system as being a major problem, or have we had a major problem with people being able to access that information when you needed it?

Mr. STREUFERT. Well, of course, the information that we draw upon to protect the borders comes from a combination of systems, including those that originate from the consular officers and our embassies and consulates and domestic locations, and that information is——

Mr. BILBRAY. Let me interrupt you and just tell you, as somebody who crosses the border probably more than most would prefer and coming in port of entries, the system from the immigrant's point of view is absolutely fantastic.

In fact, I really think, Madam Chair, we ought to be talking about allowing Americans to voluntarily go into that system of using the biometrics, whatever, because you have American citizens lining up, waiting to be interviewed, but you have a great system where foreign nationals, because they are pre-cleared, the biometrics are there, they whip right through.

So I just have to tell you, from observation, it really seems to be very much appreciated by the foreign nationals.

Mr. STREUFERT. Thank you, sir. Of course, we endeavor to make it as customer-friendly as we possibly can balanced against the se-

curity needs of protecting the border. The US-VISIT system is one that is actually hosted and managed by one of the elements of the Department of Homeland Security. But to your specific point, there are data exchanges between the Department of Homeland Security and the State Department, and one of the things that we try to do is to make sure that all of the systems that maintain our part of that potential handoff to Homeland Security are as well protected as possible.

Mr. BILBRAY. Because if you don't do it right, when they fly into the airport, that system is going to have a problem.

Mr. STREUFERT. Exactly.

Mr. BILBRAY. Thank you very much.

I yield back, Madam Chair.

Ms. WATSON. Thank you.

I will yield to Mr. Luetkemeyer, if he might have questions.

Mr. LUETKEMEYER. Thank you, Madam Chair. I don't have any questions at this time.

Ms. WATSON. This is still our first panel.

Mr. LUETKEMEYER. That is very good. Thank you.

Ms. WATSON. Thank you.

All right, I want to thank all of the panelists. Thank you for indulging us and waiting around and your patience. We appreciate it. So we will not dismiss this panel and we will call up panel No. 2. Thank you so very much for your testimony.

Panel No. 2. If you will 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. Let the record reflect that the witnesses answered in the affirmative.

Now I will take a moment to introduce our distinguished panelists. I would first like to start with Mr. Philip Bond, who is the president of TechAmerica. Mr. Bond is also president of the World Information Technology Services Alliance [WITSA], a network of industry associations representing 70 high-tech trade groups around the world. Previously, Mr. Bond served as Under Secretary of the U.S. Department of Commerce for Technology, and from 2002 to 2003 served concurrently as Chief of Staff to the Commerce Secretary, Donald Evans.

Mr. Gilligan is the president of the Gilligan Group and has, for over 25 years, been in managerial services in leading large information technological organizations. Prior to joining the private sector, Mr. Gilligan served as the Chief Information Officer of both the U.S. Air Force and the Department of Energy. He also serves as a member of several boards and advisory groups, including Software Engineering Institute and the Commission on Cybersecurity for the 44th Presidency.

Mr. Alan Paller is the director of research at the SANS Institute, where he is responsible for overseeing all research programs. His work at SANS includes overseeing the Internet Storm Center and an industry-early warning system, the publication NewsBites, and participation in other collaborative efforts to identify and mitigate new and emerging cyber threats.

Mr. Christopher Fountain is the president and CEO of SecureInfo Corp., which provides information assurance solutions to both civilian and military customers across the Government. He has a successful track record of leading and growing companies, with over 22 years of experience in the information technology industry field.

I welcome all of you and I ask that each one of our witnesses now give a brief summary of their testimony and please try and keep your summary under 5 minutes in duration, if you can, because your complete written statement will be included in the hearing record. So, Mr. Bond, would you please proceed? And thank you for being here.

STATEMENTS OF PHILIP BOND, PRESIDENT, TECHAMERICA; JOHN GILLIGAN, PRESIDENT, THE GILLIGAN GROUP, INC.; ALAN PALLER, DIRECTOR OF RESEARCH, SANS INSTITUTE; AND CHRISTOPHER FOUNTAIN, PRESIDENT AND CEO, SECUREINFO CORP.

STATEMENT OF PHILIP BOND

Mr. BOND. Thank you, Chairwoman Watson and Ranking Member Bilbray. Thank you very much. I was privileged to testify before you in 2007 on this subject, to say that it was time to focus on results rather than compliance, and thrilled to hear that is exactly the focus of your draft legislation. Two and a half years after that, with some more consultation in the meantime, we are very much looking forward to FISMA 2.0.

Today, I want to offer an updated version of the recommendations I made 2½ years ago, because we think they are still pertinent. But first I want to acknowledge the new era that we are in, unprecedented attention at the White House, from Federal CIOS, and here on Capitol Hill; the White House, of course, with the new Cybersecurity Coordinator. TechAmerica, yesterday, released its 20th survey of Federal CIOS. Their No. 1 strategic issue: cybersecurity. And here on Capitol Hill, more than 12 active cybersecurity bills under consideration right now.

I am proud to say, on behalf of our members, the industry has responded with companies coming forward with new solutions, new technologies faster than ever before, and with their clients addressing the needs to manage risk and enhance collaboration with industry partners. Examples would be Lockheed Martin's new Cyber Security Technology Alliance, Microsoft's leadership in taking down the Waledac Botnet, and the private sector's quick response on the Conficker worm, exhibiting exactly the kind of nimbleness that they offer to their partners in the Federal Government.

So we commend the Chair in taking this important step and focusing again on actual security, not just compliance.

Let me mention the six reforms that we have updated and think are still relevant.

One is to reform the agency information security approval process, that is, the way they work with private sector partners to make sure that it is as uniform as it can be.

Second, to remove barriers to innovation. This is what Vivek Kundra referred to as the culture of compliance, which makes a

culture which is not welcoming to new approaches, because if they can use a time-tested one and check the box, that complies, but it doesn't necessarily embrace the new innovative solutions.

Third, we would say increase accountability and authority for the CIOS and Chief Information Security Officers, CISOs, and to provide a forum where they can collaborate regularly.

Fourth, we agree with the need to enhance Federal cyber risk management. You heard a great example from the State Department. This would mean, by the way, more security clearances for information security professionals, more agencies with real-time access to some of the classified information, because you don't know what you don't know.

Fifth, we need to harmonize and enhance the audit and oversight methods used, thinking primarily of IGs here. You need to make those processes as uniform as you can so that it is not terribly different; and then, of course, that they are informed on what is a very technical subject, as they are doing their reviews.

Sixth, we would urge expanding Federal cyber response capabilities, and that would mean codifying and improving the standing of US-CERT and helping to pave the way for what we think, from the industry side, is very important: co-located, meaning working side-by-side, the best of the private sector and the best in the public sector, to address this national challenge.

In closing, I would just note that FISMA is now almost 8 years old. The reform has been in discussion for a number of years. And while the ideal is always a comprehensive bill addressing all aspects of cybersecurity, that can be a great legislative challenge. So we would just observe and acknowledge that we don't want the perfect to be the enemy of the good, and if we get late in the session, we would urge that FISMA reform not wait. And we believe, to use Mr. Bilbray's terminology, with a little more perfection, the tiers bill would be great progress. Thank you.

[The prepared statement of Mr. Bond follows:]

TechAmerica
WHERE THE FUTURE BEGINS

TechAmerica.org

601 Pennsylvania Avenue NW
Suite 600, North Building
Washington, DC 20004
P 202.682.9110 F 202.682.9111

Statement of

Phillip J. Bond
President and CEO
TechAmerica

Concerning

Federal IT Security: The Future for FISMA

Before the

Subcommittee on Government Management, Organization, and Procurement

Committee on Oversight and Government Reform

U.S. House of Representatives

March 24, 2010

Good afternoon, Chairwoman Watson and Ranking Member Bilbray and Members of the Subcommittee. My name is Phil Bond, and I am President and CEO of TechAmerica. Thank you for giving me the opportunity to present the tech industry's views on federal IT security and the future of the Federal Information Security Management Act (FISMA).

TechAmerica is the leading voice for the U.S. technology industry, which is the driving force behind productivity growth and jobs creation in the United States and the foundation of the global innovation economy. Representing approximately 1,200 member companies of all sizes from the public and commercial sectors of the economy, it is the industry's largest advocacy organization. It is also the technology industry's only grassroots-to-global advocacy network, with offices in state capitals around the United States, Washington, D.C., Europe (Brussels) and Asia (Beijing). TechAmerica was formed by the merger of AeA (formerly the American Electronics Association), the Cyber Security Industry Alliance (CSIA), the Information Technology Association of America (ITAA) and the Government Electronics & Information Technology Association (GEIA).

TechAmerica's track record in addressing issues related to information security is well documented, and we maintain a robust program specifically focused on the area. Additionally, many of our member companies provide information technology, managed security and systems integration services to the federal government. We have been involved in efforts to improve information security in departments and agencies for over a decade, including our support for FISMA when it was originally proposed. This hearing sends a clear signal that you understand that information technology – and its use – is not static and that we must continually assess our needs and capabilities. In the same way, information security is not a snapshot in time; just as our information technology needs evolve over time, so do the threats to and vulnerabilities in our ever-advancing information infrastructures. Given this dynamic environment, it is our collective responsibility to continue to assess those needs; to update the mechanisms we are using to assess our risks; and to ensure improvements in the security of our government networks.

When I testified before the Subcommittee in 2007 on this topic, I highlighted the key benefits of FISMA; addressed the state of information security in the federal government and identified specific challenges; discussed the roles and responsibilities of IT solutions providers; and provided a set of recommendations for enhancing FISMA, both in policy and in practice. In my testimony today, I would like to take the opportunity today to reiterate and elaborate on those recommendations in today's context.

Today's Context

What has changed since 2007? In a way, 2007 was a watershed. Estonia went globally public about the cyber attacks it experienced, as did Georgia, and the U.S. Government publicly acknowledged it had experienced intrusions in its networks as well. The U.S. Government reacted swiftly and strongly...more so than it had ever before in the area of cybersecurity. It

launched the Comprehensive National Cybersecurity Initiative (CNCI), the whole intent of which was to better protect it networks and systems. Since then, the incoming President quickly called for a review of our national cybersecurity policy framework. I was privileged to be at the White House for the President's historical speech on cybersecurity on May 29, 2009 when he released the results of that review and, importantly, announced the pending appointment of a cybersecurity coordinator in the White House. There are no less than 10 cybersecurity related bills pending before Congress, and more to come. There is more attention and momentum on cybersecurity right now than we have ever seen. At the same time, we know that attacks are still happening, and they are still growing in number and sophistication. And, we know that government systems and networks are still targets for malicious actors. Therefore, we need to take action on shoring those assets up, and updating FISMA can help do that.

Recommendations for Updates and Improvements

There are six areas of FISMA and federal agency information security that we identified for updates and improvements. The adjustments may be in the law itself in some cases, and in implementing guidance or agency policies and procedures in other cases. They all touch upon some aspect of greater governance of information security management in the agencies. The following is a recap of those recommendations and updates to our perspective on the progress we have made or where additional improvements that have been identified.

Reform Annual Agency Information Security Program Approval Process

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

In reality, the disparity among agency information security programs and policies can create confusion when it comes time to contract for services. For example, Section 3544 outlines Federal Agency Responsibilities for the head of the agency, which includes "...information collected or maintained by or on behalf of the agency."[1] While the language in the law seems clear about the agency head responsibilities, including those services provided by contractors, it is not always clear in practice. We believe that clarification and harmonization of contractor roles and responsibilities related to supporting FISMA requirements – could improve consistency among contracts and improve government security among the agencies.

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

Update: We still believe that we can do more to clarify and harmonize contractor roles and responsibilities to improve consistency – and some predictability – in contracts for government security.

Remove Barriers to Innovation

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

Update: We still believe that in practice, there is resistance to the adoption of technologies on a timely basis by government agencies. In today's context, we know that many agencies are grappling with how – and if – they can leverage cloud computing services in their systems, for example. While there may be reasons to use it and times when you may choose not to, it should not be because that box is not on the so-called FISMA checklist. To the extent that legislation can provide a mechanism that enables agencies to seek out innovative approaches that would be an improvement.

Increase Accountability

Third, it has been more than 10 years since the Clinger-Cohen Act amended the Paperwork Reduction Act and created the CIO position for federal agencies and established capital planning and investment control and performance and results-based management.[2] In 2004, GAO reported on the evolution of the CIO's role and recommended that Congress further investigate the need to reform or modernize the role of the CIO. We believe that in addition to modernizing the role of the CIO, federal Chief Information Security Officer (CISO) positions need to be studied and rationalized to ensure that both the CIO and the CISO are organized, authorized, and funded to ensure that the agency head maintains the accountability that FISMA requires. For example, an agency CIO may not have clear budget or operating authority. Additionally, the CISO most often does not have sufficient authority or integration into the senior management of an agency. If we look at the private sector, we can see some clues about how to address this concern. We are seeing an evolution toward a more active CISO in the senior management structure of an organization who is more fully engaged in the risk management and security decisions of the corporation.

This is a paradigm that should be reflected in the organization of every agency's senior management ranks. Homeland Security Presidential Directives 7 and 12 (HSPD-7 and HSPD-12) both reinforce the need to bring the key components of security leadership together to address strategies in a cohesive, integrated manner by addressing the need to bring the cyber,

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

physical, and personnel components of the risk spectrum together. A strengthened FISMA could help to break down current silos and make coordinated management decisions that can more fully permeate the organization. We need to give flexibility to agencies to determine how best the information security component fits into their operations, while bringing the function into a senior management role and, ideally, providing the commensurate budgetary and resources authority to that function and its obligations. From the private sector perspective, it appears that FISMA is not being effectively reinforced through the authorization and appropriations process, and we think that connection could make a significant improvement in the implementation of FISMA requirements and information security programs. TechAmerica believes that the agencies, OMB, the authorizers, and the appropriators could more closely coordinate their approaches to information security to ensure that effective investments are proposed and made, with appropriate consequences for inaction.

Update: While there is still not a formal mechanism to ensure the authorities and responsibilities of agency CIOs or CISOs, we have seen improvement in the way agency CISOs integrate into management roles and make progress. For example, the Department of State's John Streufert has successfully pursued and implemented a risk scoring system that is well underway in the Department and well regarded by his peers – and policy makers. In order to secure such success throughout the government and over the long term, however, we continue to believe that updates to FISMA should include a mechanism ensuring the appropriate authority for CIOs and CISOs with commensurate accountability in their organization. Additionally, we believe that it is important to provide a forum for CIOs and CISOs to meet regularly and share experiences, expertise, information, and best practices that can help inform the peer group and foster harmonization at the earliest possible stage.

Enhance Federal Cyber Risk Management

Fourth, a greater understanding of the threat to the information security in the federal agencies is a key element to an improved risk management approach. Today, some federal agencies are operating in the dark. They have not incorporated unclassified information into a risk assessment, and they do not have adequate access to classified briefings, or the classified communications capabilities necessary to receive sensitive information on a timely basis. An updated FISMA should articulate the need for at least an annual federal government information security risk assessment incorporating required assessments by the federal agencies. Those assessments should encompass both unclassified and classified information and should also include input from the private sector, as many companies have deep insight into network activity, the overall health of the Internet, and the constantly evolving threats to agencies, businesses, and individuals in cyberspace. That requirement would compel the agencies to identify relevant staffing and resource needs and, as a result, better understand how to mitigate the most urgent risks.

We also need to embrace a true risk management approach. We know we cannot achieve perfect security – for either information or physical assets. Therefore, the decisions that agencies make need to reflect risk assessments that prioritize the threats based on the potential

consequences of inaction. This will compel more rigor in the risk assessment process in the agencies, encourage preventative measures rather than merely reactive measures, and thereby improve the federal government's overall readiness.

Update: We continue to believe in a risk management approach that includes greater situational awareness in the agencies about the threat, including input from the private sector. We understand that agencies have increasing access to classified information, which is a positive trend. We think that more needs to be done, however, to ensure continual situational awareness for the agencies' operators. In addition, any performance or reporting measures should accommodate a risk management approach.

Harmonize and Enhance Audit and Oversight Methods

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

Update: We continue to believe that more uniform and informed assessment of agency information security measures is critical for success. This includes a consistent measure for security that can be applied from one agency to another, a consistent baseline for new approaches that may be adopted going forward, and, importantly, a greater consistency in the audit/investigative functions.

Expand Federal Cyber Response Capabilities

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

approach over time, it can also help improve the day-to-day operations of the very response center upon which the agencies rely.

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

Update: We see improvement in the federal incident response capabilities, though we know there are still challenges that hamper US-CERT's abilities. For example, when the Conficker worm was promulgated, industry had coalesced around its own incident response mechanism – however ad hoc – much more quickly than the government was able to do. We believe that we should look very hard at how best to improve the structure and operations of US-CERT, including how governance issues and how both industry and government would benefit from a co-located operational environment with experts from both segments working together on an on-going, sustained basis for real-time analysis and collaboration.

Role of the White House, OMB and NIST

The Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have important roles to play in the information security of federal agencies. OMB holds the purse strings, and the Chief Information Officer is a key collaborator in determining the most productive and efficient approaches for the agencies. We encourage OMB to look at ways to fund innovation security ideas in the agencies so they can keep up with technology and with the ever-evolving threat environment. NIST provides standards and guidance to the agencies on how they can achieve their information security objectives. We greatly appreciate the ability for industry to participate with NIST in the development of their publications, as industry representatives have insight and expertise that is beneficial to those deliberations. For example, our member companies have technical experts participating right now in the global supply chain and the smart grid work at NIST that will directly impact the agency activities. We would encourage NIST to continue to recognize private sector best practices for information security as a building block for federal information security and to look at new ways that agencies can change their processes to encompass prioritization of controls and continuous monitoring throughout the security lifecycle.

We have long advocated for a senior level cybersecurity position in the White House, so we were very pleased with the President's establishment of a special advisor and cybersecurity coordinator position and cybersecurity office in the White House. One of the roles of that office should be to coordinate and help improve cybersecurity in the agencies through a certain level of oversight, facilitation, and governance that is appropriate to that office as it implements the recommendations of the Cyberspace Policy Review.

Conclusion

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

Ms. WATSON. Thank you so much, Mr. Bond.
We will proceed to Mr. Gilligan.

STATEMENT OF JOHN GILLIGAN

Mr. GILLIGAN. Good afternoon, Chairwoman Watson and Congressman Bilbray and members of the subcommittee. I would like to thank you for this opportunity to address the committee and congratulate you, Chairwoman Watson, for the Federal Information Security Amendments Act of 2010. I believe it is an important step in the Nation's efforts to provide the secure and reliable information technology enterprise that we need.

Like many of you, I have a personal sense of urgency for making dramatic improvements in cybersecurity in the Federal Government. This sense of urgency is informed by the growing threat to our way of life, resulting from fundamental weaknesses in the computers and networks that have become the foundation of our Nation's prosperity. I have watched over the past decades as our cyber threat has grown steadily and the pace of our ability to protect against these threats has continued to be slowed by a lack of attention and, in many cases, poorly focused efforts. I believe the subcommittee's proposed legislation contains the key focus areas needed to make rapid progress against the growing threat. Before I describe these elements, I would like to characterize some of the aspects of the current cybersecurity problem as background.

First, I would acknowledge that the Federal Information Security Management Act of 2002 was a positive step in improving Government security. The law established the imperative for Federal managers to put strong emphasis on cybersecurity and highlighted the need to use a risk-based approach to identify and implement minimum security controls.

While the FISMA had many positive elements, the implementation of FISMA has been less than fully effective. For example, rather than focusing on minimum controls as required by the law, OMB policy guidance to Federal agencies has been to implement the entire catalog of controls, over 300 separate controls, published by the National Institutes of Standards and Technology. This is not possible for any Government agency of any size, and has resulted in a scattershot approach to improving security.

Moreover, the strong desire to measure and to assign grades to Federal agencies has resulted in placing emphasis on characteristics that can be easily measured, rather than on controls and activities that best reflect effective security. As a result, in general, the required FISMA metrics were manually generated, had little correlation to actual security, and were costly to produce. In addition, the areas emphasized in the metrics did not encourage investments or improvements that would have long-lasting improvement and security, such as improved used of automated controls.

Unfortunately, the implementation of FISMA has been like getting on a treadmill as a means to get to a destination. A treadmill is great if all you want is exercise, but it is not a good way to reach a destination. To continue the metaphor, in the implementation of FISMA, the Federal Government has certainly burned a lot of calories, but we are a long way to go from reaching our destination of dramatically improving security of our Federal systems.

While total security is beyond our current reach for the foreseeable future, there are many things that we can and should do to dramatically reduce our vulnerability to attacks, especially from those attackers who are relatively unsophisticated. Studies have shown that the relatively unsophisticated attacker group constitutes the majority of current attacks, roughly 80 percent as assessed by the National Security Agency. Unfortunately, our current cybersecurity defense mechanisms in the Government today are configured so fragmented and weak that a malicious individual with virtually no computer skill can download a canned attack from the World Wide Web and can cause significant harm to cyber systems. Recent collaborative efforts among the Government and the private sector have resulted in guidance for organizations to help focus on the top security control areas and to make effective use of automation. In essence, this effort is focused on addressing the 80 percent problem of the cyber threat.

Specifically, a little over a year ago, a group of security experts from the National Security Agency and other defense organizations, the Department of Homeland Security, Department of Justice, and the National Laboratories, along with colleagues in the private sector, collaborated on the identification of the most common attack patterns against cyber systems. They subsequently identified corresponding security controls along with automated means to implement these controls. Automation is the only practical way to deal with this complex problem.

The consensus effort among these security experts produced a guideline entitled 20 Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines, and John Streufert referred to them as Consensus Audit Guidelines. This document describes the 20 most critical cyber attacks and the controls that are needed to protect against these attacks. In effect, these so-called 20 critical controls reflect the highest priority security necessary to ensure a core foundation of security for information technology infrastructure. During the past 18 months, the U.S. Department of State has implemented the 20 Critical Controls guideline and has achieved significant progress in improving effectiveness of cybersecurity.

While the 20 Critical Controls are not intended to provide absolute security, implementation of them has proven to dramatically improve the ability of complex systems to withstand the majority of attacks. Implementing good hygiene security controls such as those identified in the 20 Critical Controls or CAG has additional benefits beyond security. Specifically, these benefits include reduced help desk calls, improved operational availability and reduced——

Ms. WATSON. Mr. Gilligan, can you conclude and we will hear the other two witnesses? Because we do have your statement.

Mr. GILLIGAN. OK.

Ms. WATSON. Thank you.

Mr. GILLIGAN. The key point here is that through this focused approach you can actually improve security at reduced cost, reduce operational cost, which is what, in my former CIO parlance I call sort of a no-brainer for CIOS. The key impediments to achieving that no-brainer implementation are two: one is the need for clear policy guidance that actually focuses on the right areas and, sec-

ond, to address the cultural resistance that must be overcome in order to be able to implement effective controls at an enterprise level.

In closing, I would say, as I look at the proposed legislation, I view it addresses the right areas and will be an effective means of helping us improve cybersecurity. Thank you.

[The prepared statement of Mr. Gilligan follows:]

Written Testimony of

John M. Gilligan

To the

Subcommittee on Government Management, Organization and Procurement

Committee on Oversight and Government Reform

March 24, 2010 Hearing on

"Federal Information Security: Current Challenges and Future Policy Considerations"

I would like to thank the Subcommittee for this opportunity to testify before you today, and I would like to congratulate you on the Federal Information Security Amendments Act of 2010. I believe that this bill is an important step in the nation's efforts to provide the secure and reliable information technology enterprise necessary to ensure our economic and national security.

The perspective that I bring to the Subcommittee is from a career in the Federal government and having had the privilege of serving as a Chief Information Officer as well as a procurement official for complex information technology systems. I also have background in doing secure systems research, systems design and development, as well as consulting in cyber security prior to my government career.

Like many of you, I have a personal sense of urgency for making dramatic improvements in cyber security within the Federal government. This sense of urgency is informed by the growing threat to our way of life resulting from the fundamental weaknesses in the computers and networks that have become the foundation for our nation's prosperity. I have watched over the past decades as the cyber threat has steadily grown and the pace of our ability to protect against these threats has continued to be slowed by lack of attention and in many cases poorly focused efforts. I believe that the Subcommittee's proposed legislation contains the key focus areas needed to make rapid progress against the growing threat. Before I describe these elements, I would like to characterize some aspects of the current cyber security problem as background for my comments on the proposed bill.

Perhaps it is useful to start with the question of: "Why is it so difficult to provide security for our government computer-based systems?" To understand the answer to this question, it is important to examine the enormous complexity of the problem. Cyber attacks focus on vulnerabilities that can and do exist in every hardware and software component. For example, such components include desktop computers, network routers, servers, operating systems, data base systems, web sites, commercial applications, government developed applications, and so forth. Each Federal department has hundreds of thousands or in some cases millions of these hardware and software components. The actual vulnerabilities that become the avenues for cyber attack are contained in the logic statements that comprise each and every one of the hundreds of thousands or in some cases millions of hardware and

software components used by each government organization. Also, each of these components has an enormous number of logic statements. For example, there are well over a million of logic statements in even a simple operating system. To achieve a fully secure system, one must ensure that all of these hardware and software logic statements are both perfectly correct and that they cannot be manipulated to compromise security. This requires correctness of many trillions of logic statements. It is important to know that a single logic error can become the entry point and the pathway to successfully attack against an entire enterprise.

The problem of ensuring logic correctness for our computer and network components is one that has been addressed by the world's top scientists for a long time. Suffice it to say that we are not close to having solutions to ensure absolute correctness of the trillions of logic statements. Even if and when solutions become available, it will take a generation to replace the current systems with more secure ones. As a result, we must recognize and deal with the situation that there are many thousands of vulnerabilities that exist in our fielded hardware and software systems that can be exploited by a range of adversaries ranging from malicious individuals and criminals with modest skill levels, to organized crime and nation state actors who in many cases have greater skill levels. Moreover, the threats against our cyber infrastructure are growing in number from both highly trained sophisticated attackers as well as so called unsophisticated attackers.

The Federal information Security Management Act of 2003 was a positive step in improving security within the government. The law established the imperative for Federal managers to put strong emphasis on cyber security. The bill highlighted the need to use a risk-based approach to identify and implement the minimum controls and to establish an independent review process. I was the CIO of the United States Air Force when FISMA was enacted. At that time, I was optimistic about the benefits of the new law.

While FISMA has many positive elements, the implementation of FISMA has been less than fully effective. For example, rather than focusing on minimum controls as required in FISMA, OMB policy guidance to Federal agencies has been to implement the entire catalog of controls (over 300 separate controls) published by the National Institutes of Standards and Technology (NIST). This is not possible for any government agency of any size and has resulted in a "scatter shot" approach to improving security. Moreover, the strong desire to measure and grade Federal agencies has resulted in placing emphasis on characteristics that could be easily measured rather than on controls and activities that best reflect effective security. In general, the required FISMA metrics were manually generated, had little correlation to actual security, and were costly to produce. In addition, the areas emphasized in the metrics did not encourage investments or improvements that would have long lasting improvement in security. In my view, the implementation of FISMA has been like getting on a treadmill as a means to go to a destination, such as to go to the store, or school or church. A treadmill is great if all you want is exercise, but it is not the way to reach a destination. To continue the metaphor, in the implementation of FISMA, the Federal government has certainly burned a lot of calories, but we are still a long way from reaching our destination of dramatically improved security for Federal systems.

While total security is beyond our current reach for the foreseeable future, there are many things that we can and should do to dramatically reduce our vulnerability to attacks, especially from those attackers who are relatively unsophisticated. Studies have shown that the relatively unsophisticated attackers group constitutes the majority of current attacks--about 80%[1] of all attacks as assessed by the National Security Agency. Unfortunately, our current cyber defense mechanisms are currently so fragmented and weak that a malicious individual with virtually no computer skill can download a "canned" attack program from the World Wide Web and can cause significant harm to cyber systems in government and industry.

Despite spending literally billions of dollars spent each year to improve security of cyber systems in the Federal government, we have not been able to implement the basic safeguards that can address what has been assessed as the majority of the threat, the relatively unsophisticated attacker. The root causes for this failure in my view are the following. First, we have not provided sufficient focus for our government security investments preferring instead to let individual organizations determine where to make investments. Given the complexity of the cyber problem just described and the enormous difficulty of assessing cyber attack risks, it is not surprising that this approach has resulted in well intended but poorly focused efforts in most government agencies. Second, the government has been slow to take advantage of available automation in a coordinated manner. Sure the government has bought lots of tools, but their usage is poorly aligned and not integrated. This has resulted in major gaps in security that have become the avenue for attacks. And third, we have relied far too heavily on manual methods to monitor and evaluate technical aspects of cyber security when the complexity of the government cyber environment makes these manual methods ineffective.

While we don't have the ability to produce totally secure systems, we do have the ability to implement the basic safeguards needed to protect our cyber systems from the relatively unsophisticated attacker—the 80% portion of the threat. Recent collaborative efforts among government and the private sector have resulted in guidance for organizations to help focus on the top priority security control areas and to make effective use of automation. In particular, a little over a year ago a group of security experts from the National Security Agency and other Defense organizations, the Department of Homeland Security, the Department of Justice, and the National Laboratories along with private sector security organizations collaborated on the identification of the most common attack patterns against cyber systems. They subsequently identified the corresponding security controls along with the automated means to implement these controls. This collaborative consensus effort among these experts produced a guideline entitled "20 Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines"[2]. This document describes the 20 most frequent cyber attack patterns and the controls that are needed to

[1] Testimony of Richard Schaeffer, Jr., Director Information Assurance Directorate, National Security Agency, Senate Judiciary Committee's Terrorism and Homeland Security Subcommittee, November 17, 2010

[2] Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines, http://www.sans.org/critical-security-controls/

protect against these attacks. In effect, these so called '20 Critical Controls' reflect the highest priority security controls necessary to ensure the core foundation of security for our information technology infrastructure. During the past eighteen months, the United States Department of State has implemented the 20 Critical Controls guideline and has achieved significant progress in improving the effectiveness of cyber security department-wide. Other government agencies are beginning to follow the example set by the State Department.

As just noted, the 20 Critical Controls focus on a foundational of controls for our computer and communications systems. While these so-called "good hygiene" control areas will not ensure that the trillions of logic statements are absolutely correct, they provide a solid foundation level of security needed to thwart relatively unsophisticated attackers--the 80% of the problem. These controls include such things as maintaining an accurate and automated inventory of hardware, software, and external connections. Without such an inventory, malicious devices or software can be introduced into government systems disrupting operations or compromising security. Another control is ensuring that the configurations for hardware and software products are set to enable security features and disable potential vulnerabilities. This control area expands on the very successful Federal Desktop Core Configuration (FDCC) initiative. The FDCC was initiated by the United States Air Force to take the "out of the box" operating systems from Microsoft and ensure that the many hundreds of optional settings were securely enabled. Over 600 settings comprise the FDCC. These settings ensure that attackers do not have easy access to break into the system. And while the FDCC is a good start, we need to duplicate this effort for every other software and hardware component as advocated in the 20 Critical Controls. Other controls in the 20 Critical Controls guideline address system administrator privileges, performing vulnerability assessments, implementing boundary and connection defenses, and controls over wireless devices.

While the 20 Critical Controls are not intended to provide absolute security, implementation of them has proven to dramatically improve the ability of complex systems to withstand the majority of attacks. As a result, implementing this foundation or "good hygiene" not only dramatically reduces the impact of cyber attacks, but also permits our cyber defenders to focus their energy on countering the smaller number of attacks from sophisticated adversaries. To me this is a prudent approach to make rapid progress in improving our cyber defenses.

Implementing good hygiene security controls such as those identified in the 20 Critical Controls has additional benefits. Let me illustrate some of these benefits. When an organization implements an automated capability to register and enforce tracking of software and hardware components, also called 'asset management', agencies are better able to manage expensive license agreements and to accurately manage their inventory of cyber devices. As another example, when organizations use so called "locked down" configurations such as FDCC and automated tools to ensure continuous enforcement of these configurations, help desk calls are dramatically reduced and system availability is increased. Related automated methods used to distribute software patches for these locked down configurations dramatically reduces the demand on network and system administrators, permitting personnel reductions and significantly reduced system down time. The bottom line is that a cyber system that implements good hygiene through a solid foundation of controls is a lot cheaper to operate.

In fact, my experience in the Air Force convinced me that implementing good hygiene such as the controls reflected in the 20 Critical Controls has such a positive impact on cost of operations that the security benefits are achieved with cost savings—not additional costs. This raises the question of why any CIO or government manager would not immediately rush to implement these controls. After all, implementing the controls gives you better security, better system availability, and lower cost. For me, this is an example of the "ultimate no brainer" for a CIO.

If this is such a "no brainer", then why have government and industry organizations not been more aggressive to implement these controls? The answer I assert is twofold. First, all organizations, but in particular in government organizations, are unwilling to deviate from policy mandates. As an example, if OMB mandates paper reports from departments and agencies and is publishing 'grades' based on the paper reports, a CIO better ensure that he or she has the required paper reports. The solution in this case is to ensure that the policy mandates focus on the right things.

A second reason for the failure to implement these controls is a bit more subtle. Implementing a disciplined cyber environment such as suggested by the 20 Critical Controls will result in the lessening or elimination of autonomy of individual users as well as local system and network administrators. No longer can users download software which may or not include malicious code when they desire. Also, local administrators can no longer tinker with the configurations to "optimize" the system. These and other common practices degrade overall security across the enterprise by introducing vulnerabilities that are exploitable often by even the most unsophisticated attackers. However, removing this autonomy from users and local administrators goes to the heart of the culture surrounding computer technology. Most users think that they should be able to control their computer. After all, wasn't the first desktop appropriately called the 'personal computer'? Likewise, local administrators believe that they know best how to operate and secure local systems to meet their local mission needs. This is not the case of individuals being malicious, nor is this cultural phenomenon unique to government. Very strong leadership is required to counter this cultural resistance in order to implement an organization wide cyber environment that provides the disciplined foundation controls that are called for in guidelines such as the 20 Critical Controls. The most senior officials in government organizations must unequivocally endorse these changes to overcome the cultural resistance.

The proposed legislation does an excellent job in responding to the needs for improving the security of our Federal government systems. Putting the focus for coordinating our Nation's cyber security in the White House, in the National Office for Cyberspace (NOC), ensures that we have the focused attention on cyber security and leadership from the most senor levels in government to help overcome organizational and cultural resistance. Moreover, the proposed Federal Cybersecurity Practice Board provides the necessary expertise and authority to help the Director of the NOC develop effective policy guidance and standards. I acknowledge that NIST has done an excellent job of developing guidelines. What is needed at this point is policy to focus government organizations on how to apply the NIST guidelines. The emphasis in the bill on minimum controls and the use of automation to continuously monitor the controls is both properly aligned and much needed. Finally, the bill addresses an often overlooked area, the need to leverage the power of the government acquisition buying power to require dramatic improvements in the security and reliability of software and hardware products. As we found

with the FDCC, this type of action not only results in improved products for the Federal government but more secure products that can be purchased by the private sector as well.

In summary, I would again emphasize that while total security is beyond the state of the art, there are a number of practical and cost-effective approaches that can be taken to mitigate the majority of attacks against our government cyber systems. The State Department and other organizations have provided positive examples of both enforcing a baseline of technical controls as well as the leadership approach necessary to overcome cultural resistance. The proposed bill adds key responsibilities and structure that are necessary to complement existing government authorities. It also provides the appropriate and necessary focus to make rapid progress to get ahead of the rapidly growing cyber threat. We will be well served if Congress passes this bill.

Ms. WATSON. Thank you so much.
Mr. Paller.

STATEMENT OF ALAN PALLER

Mr. PALLER. Well, this is a good day in cybersecurity, so thank you for inviting us. I wanted to tell you about something separate from this that is going on in California this weekend related to cybersecurity, and then we will do the other. The Governator and Senator Feinstein announced in October something called the California Cyber Challenge, which was an attempt to find the very talented hackers who can be part of the defense.

Just last week the CNO, the Chief of Naval Operations, announced that he was going to have five scholarships for the kids, full scholarships, full ride for the kids who did best in these competitions; and there is going to be an announcement this weekend that there will also be, in honor of you, the Watson Prize, which is for the kid who comes from Los Angeles County who does best on the whole statewide competition; and they said they would continue it as long as you were able to give it. So I hope you will.

You heard a lot of testimony about what is wrong and where we are going. I want to be very specific because you can't fix this in the general case; you have to fix it in the specific case. The law that was written probably wasn't a bad law, but it had enough bad elements in it that it enabled four terrible institutions to be created in its name. And what I mean by terrible is that whatever you do in legislation, you want to enable the defenders to be able to act at least as quickly as the offense, because if you hobble them, then we just don't have a chance. And the old law actually created four processes that hobbled them, and we actually now have proof.

You heard Mr. Gilligan talk about these 20 Critical Controls at NSA and DHS, who really know the attacks, said those are the ones you have to have. We mapped them against each of the four processes that were instituted in the aftermath of FISMA and none of them look for it. Including the FISCAM, which is the thing that the GAO and the IGs use. They all look for things that were important 10 or 12 years ago and miss the current attacks. So I don't need to take a lot of time to say your bill really makes a difference.

I would be happy to answer your questions.

[The prepared statement of Mr. Paller follows:]

Testimony of Alan Paller

Director of Research, The SANS Institute

Before the

Subcommittee on Government Management, Organization, And Procurement of the

Committee on Oversight and Government Reform

Hearing on

"Federal Information Security: Current Challenges and Future Policy Considerations"

March 24, 2010

Introduction

Chairwoman Watson and Members of the Subcommittee, this is a banner day for information security in government. After more than a decade of waste and lost opportunities caused by flaws in the legislation, the changes you are considering today promise to transform federal information security.

One of the most important goals of any federal cyber security legislation must be to enable the defenders to act as quickly to protect their systems as the attackers can act. We call this continuous monitoring and it is single handedly the most important element you will write into the new law. Continuous monitoring enables government agencies to respond quickly and effectively to common and new attack vectors. The Department of State has demonstrated the effectiveness of this security innovation. Most major corporations use it. This model is the future of federal cyber security. As our response to attacks becomes faster and more automated, we will take the first steps toward turning the tide in cyberspace, and protecting our sensitive information. The original FISMA did just the opposite – it slowed down every process and took key resources away from projects that would allow agencies to act and react more quickly. What you're considering today is not just a new way of doing security, it's a new way of thinking about security; the right way, the only way to win.

I am Director of Research for the SANS Institute, the primary training organization for the front line technologists who battle every day to protect the computer

systems and networks in the global infrastructure. SANS alumni, more than 118,000 in all, are the intrusion detection analysts, security managers, security auditors, firewall analysts, system and network administrators, incident handlers, forensic analysts, and law enforcement officers in government and industry. Their responsibilities include building, maintaining, and auditing their organizations' cyber defenses, fending off attackers, and, when attackers succeed, investigating the crime, tracking down the criminals, and correcting flaws that allowed the attack to succeed. We also run the Internet Storm Center, an early warning system for the Internet, publish the industry's authoritative list of critical new vulnerabilities discovered every week, and develop the consensus of the most damaging new attacks that agencies and companies will face in the coming year.

SANS alumni are the front-line warriors in the constant fight against cybercrime and cyber espionage. Every day, they fight to maintain control of the systems that operate our government and our economy and provide the essential services on which we all depend. The effectiveness of security practitioners who understand how to fight back against cyber attacks have been sorely hurt by FISMA-enabled processes forcing their agencies to spend more on compliance than on actual security. In my testimony today, I will illuminate the multi-billion-dollar errors that were made in the name of FISMA (the Federal Information Security Management Act) and thereby show how critically important your proposed changes will be.

I do not want to over emphasize the war-like nature of the fight, but it does resemble an arms race in that each time the defenders build a new wall, the attackers create new ways to scale that wall. Cyber warfare is not like conventional warfare. In conventional warfare deployment takes time and money and is quite visible. In cyber attacks, when the attackers find a new weapon, they can attack a few key machines or millions of computers, and successfully infect hundreds of thousands, in a few hours or days, and remain completely hidden.

Four terribly damaging processes were institutionalized in the aftermath of FISMA and GISRA (the Government Information Security Reform Act that predated and is essentially the same as FISMA). These wasteful processes slowed down our defenses and threw away billions of dollars that were acutely needed to protect systems. They forced federal chief information officers to defer investments in enterprise security because their security budgets were being consumed buying 3-ring binders full of reports that were out of date when delivered and had no discernible impact on security.

To implement GISRA and FISMA, the government created a and audit process that regularly results in misleading reports to agency heads and Congress. That flawed process was adopted by the Inspectors General, as well, who also are producing reports that answer the wrong questions.

GISRA and FISMA rewarded ineffective behaviors and created a cadre of people who call themselves security professionals but who proudly admit they cannot implement security settings on systems and network devices or find a programming

flaw. Most of these paper-warriors have no depth of understanding of current threats, cannot do an effective risk assessment, nor select the right controls to protect systems against the increasingly sophisticated attacks.

If the federal government were the only organization being impacted by the FISMA-flaws, that would be bad enough. But increasingly state governments, radically short of money, are being forced to spend scarce funds on reporting rather than security. Even worse, the electric power industry has been caught up in the culture of compliance created by FISMA. The head of security at a major southern power company told me last Friday, "I had to hire a writer rather than a security person because writing compliance reports is seen by management as more important than actually securing the systems." FISMA has perturbed the entire security job market. In the federal contractor community, writers who know a few words about security and federal regulations now make 50-80% more money than the people who actually secure systems and networks and applications. It is as if we paid the compliance staff at a hospital more than we pay surgeons. The best and brightest technical people are being forced into compliance roles because they want to keep their jobs and earn more money.

This wasteful behavior had to stop. Your new bill will go a long way toward stopping the damage.

Flawed Processes

The four processes that were created in the aftermath of FISMA and caused so much waste were:

(1) The FISCAM (Federal Information System Controls Audit Manual) audit process.
(2) The annual report process implemented by CIOs and IGs under FISMA.
(3) The certification and accreditation report-writing process.
(4) The security controls assessment process under Special Publication 800-53.

In each of these areas the authors knew their work needed improvement and they made small positive steps over the past year, but the FISMA language kept them from making the big steps needed to make federal information security effective.

The damage done by numbers 2, 3, and 4 have been well documented elsewhere. For example Senator Carper, Chairman of the Senate Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, said in a hearing on this same topic:

> *"one wasteful and ineffective area . . . is known as the 'Certification and Accreditation' process." "If we look at the chart to my right, we can see three years worth of reports from the Department of State, which cost a*

total of $38 million dollars. These reports would be worth the price tag if the tactics that hackers used were as static as words typed on a piece of paper. But hackers change how they attack us daily and their numbers continue to grow. Billions of dollars are spent ... on ineffective and useless reports, similar to the ones pictured here."
(http://www.votesmart.org/speech_detail.php?sc_id=505326)

Senator Carper did a great service to the country by illuminating the key problem of trying to use static and out-of-date reports to fight a dynamic adversary. This happens because the people who wrote FISMA, and the people who set up these wasteful processes did not and do know how the attacks are being carried out and how the threat is changing, so they ask the wrong questions. Their mistakes force agencies to focus resources on the wrong problems (generally problems that were most important a decade or more ago) and use up money that should have been target on more important activities targeted toward the current threat.

The one FISMA/GISRA-caused process that has not been widely discussed previously is the FISCAM audit process. GAO and the Inspectors General are powerful forces for good in this country. When they are forced by a flawed audit guide to ask the wrong questions, then they force agencies to spend scarce security money on the less important defenses, taking money away from what matters, and the country is less secure.

The following table shows evidence of how a recent FISCAM-based audit missed the most important controls. The table lists critical controls in the Consensus Audit Guidelines (CAG) published by the Center for Strategic and International Studies. These are the controls identified as most critical by the people who best understand the attacks (the NSA, US-CERT, the DoE Energy Labs, DoD Cyber Crime Center and others in government and the private sector who do the forensics to clean up after attacks and who actively penetrate systems on behalf of the nation.)

Sample Critical Controls Assessment Vs November 2009 FISCAM-Based Audit

(This is just four of approximately fifteen similar comparisons that will be published shortly with far more data, so agencies and auditors can see how to improve the processes.)

Critical Control (and sample test)	**Why It Matters**	**Was The Test Performed?**
Inventory of Authorized and Unauthorized Devices (sample test: determine how long it takes unauthorized systems to be recognized)	There is no way to manage a computer if you don't know it is there	NO
Secure configurations on operating systems (sample test: Install a	Vendors sell systems with weak configurations and	NO

system with a nom-FDCC compliant operating system and measure how quickly to agency finds and corrects the problem)	software vendors reset configurations; agencies have to harden the systems to stop attackers from do extensive damage to many systems	
Boundary defense (test: send a standardized set of benign attack traffic to random systems and test ability to block the traffic.)	Traditional firewalls do not stop the sophisticated attacks. The doors are wide open to attacks.	NO
Application Software Security (test: use both types of software testing tools on random applications to test the agency's application security effectiveness)	Federal web sites have been changed so they infected the computers of members of the public who visited the site.	NO

The Bottom Line

Both the guidance for implementing FISMA and the guidance for auditing compliance are focusing on out of date, ineffective defenses. What we need instead is a process that directs agencies to focus their cyber security resources on monitoring their information systems and networks in real time so that they can prevent, detect and/or mitigate damage from attacks as they occur. And oversight must be focused on the effectiveness of the agencies' real-time defenses. The bill that you have introduced, Madam Chair, does exactly that. Anything less continues to waste scarce resources and leaves us unacceptably vulnerable.

Thank you. I will be happy to answer any questions that you or other members of the subcommittee may have.

Ms. WATSON. Thank you so much.
Mr. Fountain.

STATEMENT OF CHRISTOPHER FOUNTAIN

Mr. FOUNTAIN. Thank you, Chair Watson, Ranking Member Bilbray, and members of the committee. First, I appreciate the opportunity to address the committee and look forward to answering questions at the conclusion.

I guess by way of background everybody has said repeatedly that the threat landscape has changed, there are more threats to our infrastructure than ever before, and that is occurring at the same time that we are more interconnected than ever before. So that is a given. So I would like to move quickly to what is strong about the current FISMA legislation.

While I agree it needs to be improved—and I will talk about the legislation under consideration specifically after my comments about the current FISMA law—I think it is important to recognize the strengths of FISMA and any effort to amend FISMA not do away with things that have been quite effective. First, the level of awareness has been dramatically increased as a result of this legislation, and the 107th Congress is to be commended for taking these steps well before the general public had any awareness of what cyber even meant or what cybersecurity was all about.

It also established a framework for accountability that is a critical component today and established more strength behind a security officer inside agencies. The most important point is that it established a framework for developing and maintaining guidance to be used by agencies in their effort to defend IT assets, and that guidance was really handed for the civilian government to the National Institute of Standards and Technology. And I have to commend NIST for the great work that they have done. The key point is NIST established a very comprehensive framework and at the same time they have allowed that framework to live. So the Consensus Audit Guidelines that have been commented upon, those are mapped now to the latest version of controls that are advocated or outlined in NIST guidance under 853.

There is one quote that I would like to attribute to Ron Ross, who is the doctor or the computer scientist at NIST who oversees this effort. He says, "There continues to be a notion that FISMA is all about paperwork and compliance. Rather, FISMA is about trying to improve the quality of information security." And I think the important point here is that FISMA is not about paperwork, it is about taking very deliberate, well thought-out measures to provide for better defense.

Now, with those things said, there certainly are areas for improvement, and I think the legislation under consideration provides some very good foundations for that. And I don't interpret the current legislation that is under consideration as a wholesale rewrite of FISMA; I see that as an enhancement to FISMA in its current form, which I again think is a good thing.

First, the one thing about current FISMA is it does not have real teeth. So the law today provides for reporting to Congress and to GAO, but there are no real consequences for failure to comply with FISMA. The legislation under consideration provides for enhanced

management and oversight and provides for a statutory means of achieving that, which I applaud in this legislation.

I do believe that the FISMA report card did lead to a paperwork train, but that was the reporting element, not the aspect of guidelines and standards that are robust and comprehensive.

Also in the proposed legislation, the creation of a National Office for Cyberspace is a very, very sound idea and a very logical step forward, and I congratulate you on that move and wish you luck in trying to move that through the legislative process. As outlined in the draft, the legislation does require or should require statutory authority in that office and, in my view, I would suggest that the committee consider placing that office within the Department of Homeland Security. And I will comment more about why that is.

In the Department of Homeland Security, that office should report to the President, to the Secretary of Homeland Security, and to the Congress directly, because this should be a function that cuts across all of Government and certainly is a Presidential issue.

In my written testimony, there is a lot of detail about how I would enhance the FISMA reporting to move it to a more metrics-based environment, as Mr. Kundra had suggested earlier this afternoon. I won't focus on that today. I would rather focus on the statutory office of cybersecurity.

Why DHS? I know in the current draft it is advocated to put that inside the White House. I would suggest at least consideration for Department of Homeland Security because, in my view, defending cyberspace is critical to defending the homeland. They are so tightly intertwined. Every mission across government requires reliable computers and networks to perform their mission. And even beyond the boundaries of government, the critical infrastructure that is managed by private sector companies, they rely very heavily on information assets.

Currently within DHS there is established today an office for Cyber Security and Communications, CS&C, and within CS&C is the National Cyber Security Division. There is a high degree of synergy between the mission sets in those organizations and the mission for the proposed office of the National Office for Cybersecurity.

I will read, just for reference, the NCSD mission, which is the National Cyber Security Division mission. "The National Cyber Security Division works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets." By definition, they are working across government or across, really, the private sector and the government to some extent, although with the government it is not their core focus today.

In my view, a National Office for Cyberspace working in concert with CS&C would provide for a very robust mechanism and set of processes to look across the entire technology landscape in America, the Government as well as the private sector, and all other elements of our infrastructure, academic and so on.

In summary, I think it is critical that there be recognition that core elements of FISMA as it exists today are very sound and it needs to be improved. I believe that the legislation under consideration is timely and necessary. I believe that the key to the new legislation is the statutory authority being placed in this office that

is being proposed and that along with statutory authority there needs to be a budget to allow that office to work effectively. And, again, in terms of Department of Homeland Security, in my view, protecting the homeland requires protection of our cyber infrastructure, and that is why I, again, would ask you to consider placing this function inside the Department of Homeland Security.

I thank you for the opportunity to present my views.

[The prepared statement of Mr. Fountain follows:]

Statement of

Christopher E. Fountain
President and CEO
SecureInfo Corporation

Concerning

Federal Information Security: Current Challenges and Future Policy Considerations

Before the

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

Christopher E. Fountain
March 24, 2010
Testimony to Subcommittee on Government Management, Organization, and Procurement
Federal Information Security: Current Challenges and Future Policy Considerations

Chair Watson, Ranking Member Bilbray, members of the subcommittee, thank you for the opportunity to provide testimony today regarding the current challenges facing the Federal government information security. My name is Chris Fountain. I am president and chief executive officer of SecureInfo Corporation.

SecureInfo is focused exclusively on providing information assurance and cyber security solutions to the Federal government. We help to secure information assets used by the Department of Homeland Security, the Department of Defense, and many other government agencies. We also provide these services to commercial organizations doing business with the Federal government.

In my testimony, I will address two primary topics: (i) what elements of the current FISMA legislation are working and should not be changed; and (ii) what changes and enhancements should be considered in future legislation.

General Background

This Committee created FISMA, and in so doing provided a framework to protect information technology (IT) infrastructure and secure data used across government. It provided this framework at a time when the general public was not aware of or concerned about information or cyber security.

Much has changed in the seven plus years since this law was enacted. Today, information systems, and the data they store, process, organize and manage, are central to everyday life and are more interconnected than ever. These "information assets" perform tasks as mundane as completing a phone call and as complex as controlling the reactor inside a nuclear power plant. They may contain something as simple as the date and time of someone's next dentist appointment or as mission critical as the launch sequence required to put a missile on target in a military engagement.

The United States government performs more critical missions enabled by networked information assets and holds more sensitive data than any other entity in the world. And, now more than ever, our adversaries actively seek to exploit our dependence on information assets. This puts an extraordinary burden on those working within and on behalf of our government and places an extremely high level of importance on securing information assets under the control of government.

When the 107th Congress established FISMA in law, it established an essential roadmap for the Federal government. While FISMA has been successful in improving the security posture of the Federal government's information assets, changes under consideration by this subcommittee are timely and critical.

What Elements of FISMA Are Working

General information security awareness – FISMA has contributed to a heightened awareness about the importance of information security and a disciplined approach to managing it. Training requirements under FISMA anchored the law's disciplined framework across government and ensured that security was a priority in any IT system's creation or evolution. The Department of Defense has taken this a step further and now requires specific certifications for those charged with management and administration of information assets.

Executive level accountability across all government agencies – FISMA holds the head of each agency and its chief information officer accountable for implementing policies and procedures to reduce information security risks. Senior information technology leaders focused on information security are now in place across government to support these efforts and report regularly the state of information security programs within their respective agencies.

Comprehensive information security standards and guidelines – A cornerstone of FISMA was to require the implementation and ongoing maintenance of standards and guidelines to be used by the Federal government to secure information systems. The National Institute of Standards and Technology (NIST) was directed to lead this effort for Federal civilian government agencies. As a result, the Federal government now possesses one of the most complete sets of information security standards, guidance and best practices available. This work has been so successful that the Committee for National Security Systems (CNSS) in collaboration with NIST has decided to utilize updated versions of the NIST framework for Department of Defense (DOD) and Intelligence Community (IC) systems. Highlighted below are two major NIST Special Publication updates that resulted from intense collaboration between members of the NIST, CNSS, DOD and IC organizations. The acknowledgements page from SP 800-37 Revision 1 document is attached as Exhibit 1.

- NIST introduced in August, 2009: Special Publication 800-53 Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations"
- NIST introduced in February, 2010: Special Publication 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems"

FISMA empowered NIST to develop and maintain a comprehensive suite of publications designed to help the United States government effectively and appropriately manage information security risk. NIST has proven it is highly effective at collaborating with government and industry to evolve as technology and threat vectors change. I strongly encourage this sub-committee to avoid proposing legislation that dilutes or otherwise negatively impacts NIST's key role as provided in current FISMA legislation.

Where Does FISMA Fall Short

FISMA reporting is too focused on compliance demonstration – Today, FISMA reporting to OMB and the Congress is about compliance demonstration, rather than about an assessment of the real information security posture of information assets used by government agencies. The distinction between FISMA in broad terms and FISMA reporting is important because some would argue that "FISMA" is a paperwork exercise and does not effectively improve an agency's information security posture. I would disagree. While the reporting process is too focused on compliance demonstration, the documentation related to key information security program elements, as required by standards and guidance driven by FISMA, is important and is central to the effective governance of information assets.

Since in my view FISMA reporting needs to be more performance-based, any new legislation should address how Federal agency information security programs are assessed or graded. This problem can be solved by developing and implementing a standardized and quantitative performance-based assessment program to determine whether information assets are truly secure. The assessment program should be performed using a priority scheme driven by mission impact and should utilize a sampling process. It should include simulated attacks as well as a deep inspection of key information security program elements. These assessments should be performed by highly skilled and credentialed assessors authorized to work across government. This would help to ensure consistency and objectivity.

FISMA lacks centralized authority and a statutory basis for assessing compliance – Today, FISMA lacks a strong enforcement and oversight mechanism, which I believe this legislation addresses through creation of an empowered, Senate-confirmed, dedicated office and senior cyber executive. In creating this office, the legislation envisions a stricter FISMA compliance discipline than exists today where no significant consequences result from inadequate agency adherence.

The previous basis to encourage compliance, in no small way, was built upon the non-statutory report card process initiated and overseen by this Committee. Congressional oversight constitutes a big stick and the impact of the report card process on agency compliance was substantial, but a statute ensures longer-term and more predictable compliance. Absent a statute and corresponding budget resources, FISMA runs the risk of inadequate enforcement, and hence, compliance. I believe the statute and Committee report card process are compatible. In fact, the Committee's work encouraged agencies to seek better grades. I would encourage the Committee to revisit that process as outlined above.

The office envisioned by this legislation, the National Office for Cyberspace, with statutory authority to work across government, is sound. It is a reasoned and needed evolution of a law whose enactment rationale is more important today than ever. In creating the office, Congress can put power in such a position and FISMA provides the framework and logical opportunity to achieve this.

Placement of such an office may precipitate debate in both the Congress and Executive Branch. I would encourage the Committee to consider placing the National Office for Cyberspace within the Department of Homeland Security. Its jurisdiction touches government-wide Federal operations, state and local

jurisdictions and the private sector as well. Cyber security is about homeland security, whether the threats be from terrorists or foreign nationals seeking mass destruction, theft of military secrets or damage to our economy through an array of imaginable and frightening scenarios. It should be noted that today DHS houses the National Cyber Security Division (NCSD). NCSD carries the charter for working with the private sector to ensure our nation's critical infrastructure is effectively resistant to a cyber attack. In addition NCSD works with our international partners as cyber security is by definition a global issue. Working together, the National Office for Cyberspace and NCSD will be well positioned to address cyber security needs across Federal, state and local governments, private sector organizations involved with our critical infrastructure, and our international partners. This, together with the Committee's legislation to create a dedicated office with an empowered senior executive at its head, offers a powerful combination of statutory authority and ability to collaborate to mitigate risks associated with information technology vulnerabilities, today and well into the future.

In summary, statutory changes prescribing standards-based performance requirements and accountability through a dedicated office and official, with regular reporting to the Secretary of Homeland Security, President and Legislative Branch will ensure discipline and compliance by agencies across government. Such an office is timely, and frankly, overdue. I am encouraged by the Committee's legislation and hope my perspective contributes to your work. This issue is of greater importance than many of us recognize. Our information assets are under attack every day. It is imperative that we make every effort to properly protect them.

Closing

Thank you for the opportunity to testify and present these views. I look forward to answering any questions you might have today or in the weeks ahead as your legislative initiative progresses.

Christopher E. Fountain
March 24, 2010
Testimony to Subcommittee on Government Management, Organization, and Procurement
Federal Information Security: Current Challenges and Future Policy Considerations

Exhibit 1, Acknowledgements from NIST SP 800-37 Revision 1

Acknowledgements

This publication was developed by the *Joint Task Force Transformation Initiative* Interagency Working Group with representatives from the Civil, Defense, and Intelligence Communities in an ongoing effort to produce a unified information security framework for the federal government. The Project Leader, Ron Ross, from the National Institute of Standards and Technology, wishes to acknowledge and thank the senior leadership team from the U.S. Departments of Commerce and Defense, the Office of the Director of National Intelligence, the Committee on National Security Systems, and the members of the interagency working group whose dedicated efforts contributed significantly to the publication. The senior leadership team, working group members, and their organizational affiliations include:

U.S. Department of Defense

Cheryl J. Roby
Acting Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer

Gus Guissanie
Acting Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance

Dominic Cussatt
Senior Policy Advisor

Office of the Director of National Intelligence

Honorable Priscilla Guthrie
Intelligence Community Chief Information Officer

Sherrill Nicely
Deputy Intelligence Community Chief Information Officer

Mark J. Morrison
Deputy Associate Director of National Intelligence for IC Information Assurance

Roger Caslow
Lead, C&A Transformation

National Institute of Standards and Technology

Cita M. Furlani
Director, Information Technology Laboratory

William C. Barker
Chief, Computer Security Division

Ron Ross
FISMA Implementation Project Leader

Committee on National Security Systems

Cheryl J. Roby
Acting Chair, Committee on National Security Systems

Eustace D. King
CNSS Subcommittee Co-Chair (DoD)

William Hunteman
CNSS Subcommittee Co-Chair (DoE)

Joint Task Force Transformation Initiative Interagency Working Group

Ron Ross *NIST, JTF Leader*	Gary Stoneburner *Johns Hopkins APL*	Dominic Cussatt *Department of Defense*	Kelley Dempsey *NIST*
Marianne Swanson *NIST*	Jennifer Fabius Greene *MITRE Corporation*	Dorian Pappas *National Security Agency*	Arnold Johnson *NIST*
Stuart Katzke *Booz Allen Hamilton*	Peter Williams *Booz Allen Hamilton*	Peter Gouldmann *Department of State*	Christian Enloe *NIST*

In addition to the above acknowledgments, a special note of thanks goes to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support. The authors also wish to recognize Beckie Bolton, Marshall Abrams, John Gilligan, Richard Graubart, Esten Porter, Karen Quigg, George Rogers, John Streufert, and Glenda Turner for their exceptional contributions in helping to improve the content of the publication. And finally, the authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, nationally and internationally, whose thoughtful and constructive comments improved the overall quality and usefulness of this publication.

Ms. WATSON. Thank you so much.

I am now going to defer to our ranking member for a final question or comment.

Mr. BILBRAY. Yes, a question for Mr. Fountain. What should the role be from here forward of NIST?

Mr. FOUNTAIN. I think if you look at what NIST has done—there are a couple of things about NIST that make it a real special entity, in my view. And we don't do business with NIST. I know what Ron Ross does because obviously what he does has a big effect on the things we do for Government. They need to play a very prominent role, in my view. They work very collaboratively across not only Government, but I know there is legislation under consideration in another committee in the House to have NIST work with international partners on establishing an international framework for cybersecurity, because, again, cyber is not a U.S. issue; it is a global issue, because everything is interconnected, it is not just inside the United States.

And NIST has a track record of being collaborative. I know they have worked and they are highly complimentary of the Consensus Audit Guidelines. They do believe that more needs to be done beyond that because addressing the top 20 vulnerabilities won't necessarily address every vulnerability, and you want to have a framework that addresses the entire landscape. But using the CAG, or the Consensus Audit Guideline as a good first step is critical.

So, in my view, they should be prominent across this issue, whether it is in the Office of National Cybersecurity or the National Office for Cybersecurity or the current CS&C, and then with international partners.

Mr. BILBRAY. Thank you, Madam Chair.

Ms. WATSON. I want to just end with this thought and then ask you to followup. What we are trying to do is to promote the notion of harmonizing security frameworks across civilian and national security systems, and lessons that you have learned in business in and outside of Government we would like to know about.

So if you could give us your further suggestions, and we hope that they relate to the bill that I have out there. We will welcome anything that you see will help us improve, and remember we are looking globally, we are looking across all agencies, and we want to improve our communication. As we improve our cyberspace technology, we want to be able to have a profile how we can make it safe. So I invite all of you to contribute. And remember this is an ongoing process; every day there is a new development, a new technology. So whatever ideas we need them so we can put them into our base. And remember we make policy, but that policy has to change to keep up with the changing times.

So I want to thank all the witnesses and Members who attended this hearing. Without objection, the committee will be adjourned.

[Whereupon, at 4:56 p.m., the subcommittee was adjourned.]

○